Kofax SafeCom Go Ricoh
Administrator's Guide

Version: 030.06.3.1

Date: 2023-05-03

KOFAX

Table of Contents

Introduction

Kofax SafeCom Go Ricoh is the internal solution for Ricoh MFPs. It integrates with the touch-screen control panel of the Ricoh MFP and offers user authentication by code and/or card. The Ricoh MFPs are also supported when sold under the Gestetner, Lanier, Nashuatec, Rex-Rotary and Savin brands.

SafeCom Go Ricoh works together with the SafeCom G4 Server software and is designed to help companies and organizations gain control over their printing costs and document security. The SafeCom solution can be enhanced with add-on modules to build customer specific and scalable solutions.

Requirements

SafeCom Go Ricoh supports all MFPs and printers listed here.
- SafeCom device license.
- SafeCom ID device license.
- MFP must be connected to the network.
- MFP/printer must have a hard disk.
- If users are to be identified by card, a SafeCom ID device needs to be installed at the MFP.
- If you are planning to use Smart Operating Panel (SOP), the following limitations apply:
  - Ensure that your SOP firmware version is 1.38 or newer.
  - Ensure that your Ricoh MFP system version is 3.11 or newer.
  - Pressing the **Home** button of the device navigates away from the SafeCom lock screen. Tap the **SafeCom Go** button on the device screen to bring up the SafeCom Go application and log in by typing your access credentials.
  - To log out manually, tap the **Logout** button in SafeCom Go.
  - You can use your card to login on any device screen, regardless of whether SafeCom Go is in the foreground.

> ⓘ During printing activity, it is not possible to scan or copy.

SafeCom Go Ricoh products

SafeCom Go Ricoh	MP C401SP, MP C401SRSP
	MP 2553, MP 3053, MP 3353
	MP C2003SP, MP C2503SP
	MP C3003, MP C3503, MP C4503SP, MP C5503SP, MP C6003SP
	MP C6502SP, MP C8002SP, Pro C5100S and Pro C5110S with Ricoh Controller only, Pro 8100S, Pro 8110S, Pro 8120S
	MP 2352SP, MP 2852SP, MP 3352SP
	MP C300, MP C400
	MP C2051, MP C2551
	MP C3001SP, MP C3501SP
	MP C4501SP, MP C5501SP
	MP C6501SP, MP C7501SP
	MP 2851, MP 3351
	MP 4001, MP 5001, SP 5200S, SP 5210SF
	MP C3002, MP C3502 MP 6002, MP 7502, MP 9002
	MP 4002, MP 5002
	MP C4502, MP C5502
	Order the license and USB ID device separately.
	Devices are supplied with Java VM card.
SafeCom Go Ricoh Type N	MP 2852, MP 3352
	Order the license and USB ID device separately.
	Java VM Card Type N is required and MUST be ordered through a Ricoh reseller.
SafeCom Go Ricoh Type L	MP 171, MP 201F, MP 201SPF
	Order the license and USB ID device separately.
	Java VM Card Type L is required and MUST be ordered through a Ricoh reseller.
SafeCom Go Ricoh Type J	MP 6001, MP 7001, MP 8001, MP 9001, Pro 907EX, Pro 1107EX, Pro 1357EX
	Order the license and USB ID device separately.
	Java VM Card Type J is required and MUST be ordered through a Ricoh reseller.
SafeCom Go Ricoh Type I	MP C2050, MP C2550, MP C2800, MP C3300, MP C4000, MP C5000
	Order the license and USB ID device separately.
	Java VM Card Type I is required and MUST be ordered through a Ricoh reseller.
SafeCom Go Ricoh Type F	MP 2550, MP 3550, MP 4000, MP 5000, MP C6000, MP C7500
	Order the license and USB ID device separately.
	Java VM Card Type F is required and MUST be ordered through a Ricoh reseller.

SafeCom P:Go Ricoh products

SafeCom P:Go Ricoh	SP C431N, SP 5210DN Order the license and USB ID device separately. Devices are supplied with Java VM Card.
SafeCom P:Go Ricoh Type O	SP C320DN, SP C430N SP 4310N, SP 5200DN Order the license and USB ID device separately. Java VM Card **Type O** is required and MUST be ordered through a Ricoh reseller.
SafeCom P:Go Ricoh Type K	SP 4210N, SP C820DN, SP C821DN Order the license and USB ID device separately. Java VM Card **Type K** is required and MUST be ordered through a Ricoh reseller.
SafeCom P:Go Ricoh Type H	SP C420DN, SP 8200DN Order the license and USB ID device separately. Java VM Card **Type H** is required and MUST be ordered through a Ricoh reseller.

SafeCom ID devices

SafeCom Go Ricoh-supported SafeCom ID devices

Identification method
SafeCom AWID Reader
SafeCom Bar Code Scanner
SafeCom Bar Code Reader
SafeCom Casi-Rusco Reader
SafeCom Cotag Reader
SafeCom EM Reader [E] SafeCom EM Reader [R]
SafeCom Felica Reader
SafeCom HID Reader 35 bit [E] SafeCom HID Reader 35 bit [R]
SafeCom HID Reader 37 bit
SafeCom iCLASS Reader [E] SafeCom iCLASS Reader [R]
SafeCom Indala Reader 26bit
SafeCom Indala Reader 29bit
SafeCom IoProx
SafeCom Legic Reader [E] SafeCom Legic Reader [R]

Identification method
SafeCom Magnetic Card Reader (Tr 1)
SafeCom Magnetic Card Reader (Tr 2)
SafeCom Magnetic Card Reader (Tr 3)
SafeCom Magnetic Card Reader DD (Tr 1)
SafeCom Magnetic Card Reader DD (Tr 2)
SafeCom Magnetic Card Reader DD (Tr 3)
SafeCom Mifare Reader [E] SafeCom Mifare Reader [R]
SafeCom Nedap Reader
SafeCom NexWatch Reader
Kofax Mx Proximity Reader
Kofax Mx Legic Proximity Reader
OMNIKEY 5x27 CK

Additional information about the ID devices is available in *Kofax SafeCom G4 Administrator's Manual* that can be downloaded from Product Documentation (kofax.com).

> ℹ️ ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.
>
> To use OMNIKEY 5x27 CK readers with SafeCom and Ricoh devices, the **Keyboard Wedge** > **Output Type** setting must be **Custom Report**.

The following documents are available on the Product Documentation (kofax.com) site.

SafeCom Smart Printing

- *SafeCom Smart Printing Administrator's Quick Guide*: How to install a SafeCom Smart Printing solution.

SafeCom G4

- *Kofax SafeCom G4 Administrator's Manual*: A comprehensive manual that the administrator should consult to make a successful SafeCom solution. Includes information about SafeCom Tracking, SafeCom Rule Based Printing, SafeCom Client Billing, and SafeCom Pay.

SafeCom Go Ricoh

- *SafeCom Go Ricoh Administrator's Manual* (this manual): A guide about how to install, configure and use SafeCom Go Ricoh.
- *SafeCom Go Ricoh User's Guide*: User's guide about how to use SafeCom Go Ricoh.

About this guide

This guide applies to Kofax SafeCom G4 Server version S82 070.530*00 and Kofax SafeCom Go Ricoh 030.06.3.1.

Chapter 2

SafeCom Go Ricoh

Make sure the SafeCom G4 Server software installation has been completed. For more information, refer to *SafeCom Smart Printing Administrator's Quick Guide* available on the Product Documentation (kofax.com) site.

- SafeCom Go Ricoh hardware installation
- Increase heap and stack sizes, and configure the diprint timeout on Ricoh device (Ricoh Device Configuration)
- Ricoh Java software installation
- SafeCom Go Ricoh software installation
- Additional configuration

SafeCom Go Ricoh hardware installation

Refer to the appropriate section:

- If the device has Java embedded, connect the USB SafeCom ID device to the device's USB port and proceed to SafeCom Go Ricoh software installation.

  ⓘ ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

- If the VM card (SD card) is supplied by Ricoh, proceed to Install the VM card supplied by Ricoh.

Install the VM card supplied by Ricoh

1. Press the operation switch to turn off power. Wait for the **On** indicator to go off (stop blinking) and then turn off the main power switch. Disconnect the power cable.
2. Locate the printer's SD card slots (typically located at the rear of the printer near the RJ-45 network socket). On some printers, you have to remove a plastic cover first.
3. Insert the SD card labeled **VM Card** in SD card slot 2 or 3.

Install the SafeCom ID device

Connect the SafeCom ID device to the device's USB port.

ⓘ ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

Reconnect power

1. Connect the power cable. Turn on the main power switch. Press the operation switch to turn on power.
   The printer's control panel displays **Please wait** for 30 seconds.
2. Proceed to Ricoh Device Configuration.

Ricoh Device Configuration

Increase Heap and Stack sizes on Ricoh device

1. Open a web browser and enter the printer address.
   JavaScript (Active Scripting) must be enabled.
2. Click **Login** and enter **Login User Name** (admin) and **Login Password** (by default, there is no password) and then click **Login**.
3. Click **Configuration** on the left menu.
4. Under **Extended Feature Settings**, click **Administrator Tools**.
5. Change Heap Size to minimum 16 MB (on Ricoh Type C, set it to 10 MB).
6. Change Stack Size to 64 KB.
7. Click **Apply**.
8. Restart the printer.

Configure the Diprint Timeout value on the Ricoh device

On select Ricoh devices released after October 2014, a device setting named "diprint timeout" has a factory default value of 15 seconds. To avoid problems using encryption when utilizing SafeCom secure printing on the device, this timeout needs to be increased to at least 300 seconds.

To change the diprint timeout setting on the device, follow the steps below.

1. Open a telnet connection to the device.
2. Authenticate with device admin credentials.
3. Enter the command "diprint" to show the current diprint timeout.
4. To modify the value, enter "diprint timeout {XXX}", where {XXX} is the timeout in seconds.
   The recommended minimum value is 300 seconds.
5. Enter the command "logout".
6. Enter "yes" to save the new diprint settings.
7. Proceed to Ricoh Java software installation.

Ricoh Java software installation

Install the Java platform:

1. Open a web browser and enter the printer's address.

   JavaScript (Active Scripting) must be enabled.

2. Click **Login** and enter **Login User Name** (admin) and **Login Password** (by default, there is no password) and then click **Login**.

3. Click **Configuration** on the left menu.

4. Under **Extended Feature Settings**, click **Install**.

5. Select **SD Card Slot**.

6. Click **Display Extended Feature List**.

7. In **Install to**, select **SD Card Slot {N}**, where {N} is the slot with the VM Card.

8. In **Auto Start**, click **On**.

9. On the **Extended Feature List**, click **JavaTM Platform.**

10. Click **Install**.

11. On the Confirm web page, click **OK**.

12. Proceed to SafeCom Go Ricoh software installation.

SafeCom Go Ricoh software installation

Send SafeCom Go Ricoh (*.b87) file

1. Make sure the printer is powered on and ready.

2. Start the SafeCom Administrator and log in to the server.

3. Invoke the **Add device** function from the **Devices** menu, the **Toolbar** button, or the **System overview**.

4. Enter the **Printer address**. Click **Next**.

   Information is retrieved from the device to establish the type of device.

5. Click **Next**.

6. On the **Settings** tab, specify the properties of the device (**Duplex supported** and **Color supported**).

7. Click **Add** to register the device and save it in the database.

8. Browse to the SafeCom Go Ricoh Software file.
   Example: 500xxx.b87

9. Click **Send** to send the SafeCom Go Ricoh Software (*.b87) file to the device. If the file is not present, you need to get the file first (Get the SafeCom Go Ricoh software).

   The printer restarts. After a few minutes, the printer's control panel says **Ready**. After another 2-7 minutes (depending on model), the control panel says **Loading SafeCom**. After 1-2 minutes more, a SafeCom login message is displayed.

10. Open the Configuration web page and then specify the SafeCom server.

Additional configuration

- How to make SafeCom stay always on top
- Enable copy control and access control to other functions
- Enable E-mail
- Enable Send to Fax
- Enable Address Book
- Enable single sign-on for Kofax DigiDocFlow

Enable SafeCom Smart Scan

The SafeCom Smart Scan feature allows users to scan a document and then manage or download the scanned files from either the SafeCom Web Interface (*SafeCom G4 Web Interface Administrator's Manual D60651*) or from the *Move (SafeCom G4 Administrator's Manual D60650*) available on the Product Documentation (kofax.com) site.

1. Open the Configuration web page (Configuration web page).
2. Scroll to the Device section and check **Smart Scan**.
3. Click **Apply**.

Configuration steps for single-function printers

For single-function printers, the following criteria must be met in addition to your specific setup:

- A login method using card-based authentication must be selected (Select user identification – user code or card).

- **Print all at login** must be enabled for the printer through SafeCom Administrator.

SafeCom Go Ricoh web interface

The SafeCom Go Ricoh web interface adheres to the structure and design of the Ricoh Embedded Web Server. The SafeCom Go Ricoh web interface consists of two parts: a public part (namely, the Information web page) and a password-protected part.

Log in to the SafeCom Go Ricoh web interface

1. Open a web browser and enter the printer's address followed by: `8080/safecom`.
   Example: `http://172.16.6.55:8080/safecom`

   > ℹ️ JavaScript (Active Scripting) must be enabled.

2. Click **Configuration** on the left menu to access the SafeCom Configuration web page. Enter user name (admin) and password (nimda). Click **OK**.

Information web page

The Information web page shows a version and configuration summary.

Click **SafeCom** on the menu to access the Information web page.
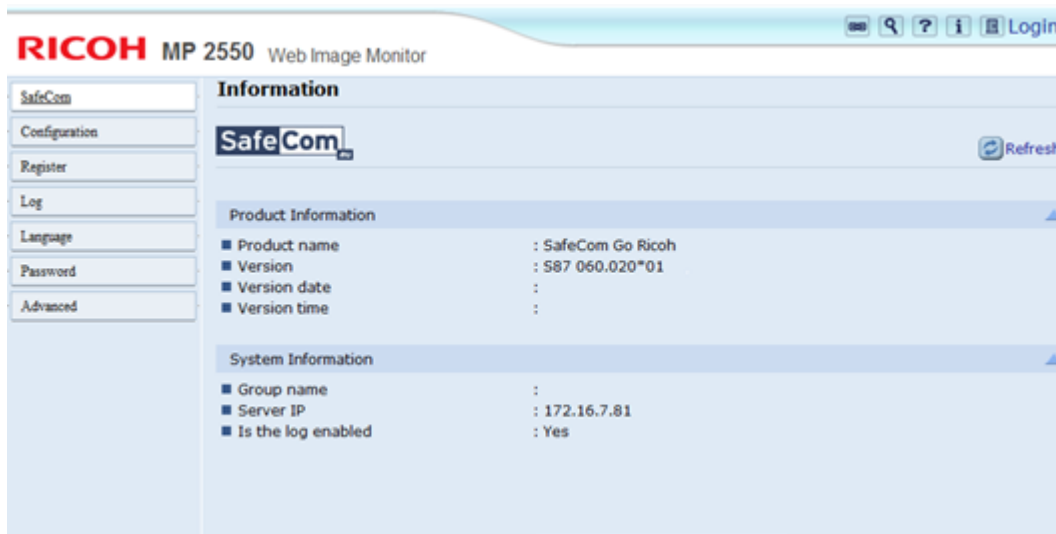
> ⓘ When the Information web page is opened, the above information and additional debug information is copied to the clipboard. The information can be pasted into an editor such as Notepad or into the body of your e-mail message by pressing Ctrl + V.

Configuration web page

Use the Configuration web page to configure your SafeCom Go Ricoh MFP, as described below. The Configuration web page for printers is described in Configuration web page – printers.

The Configuration web page for Ricoh MP 171, MP 201F, and MP 201SPF are described in Configuration web page – MP 171, MP 201F, MP 201SPF.
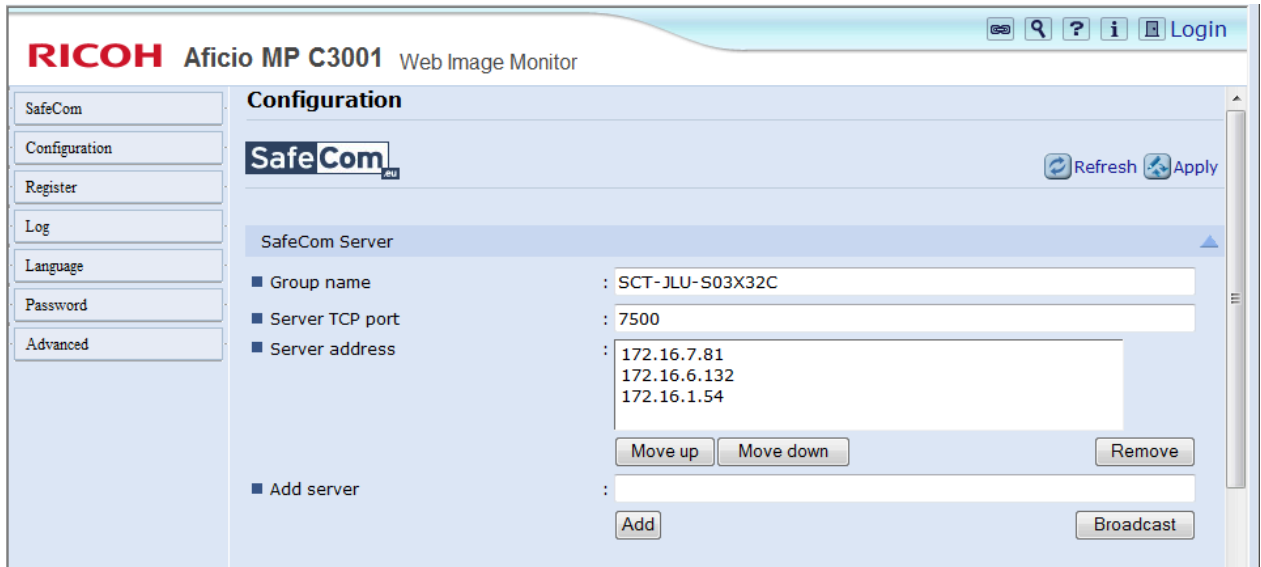
Under **SafeCom Server**, click **Broadcast** to get a complete list of servers to select from, or enter **Group name**, **SafeCom server TCP port** (default is 7500), and the SafeCom server IP address in **Add server**. See Specify the SafeCom server.

ⓘ After you click **Apply**, it takes one minute before the new SafeCom Server settings take effect. Not waiting long enough may result in a login error at the printer.

Under **Device**, enter specific details. Make sure to click **Apply** in the upper right corner when you have made your changes.

Device name and **Device model** are automatically filled-in. **Device location** and **Contact person** are important references for the SafeCom solution, so it's a good idea to fill them in.

Login method controls how users identify themselves at the MFP. In the drop-down box select an identification method:

- ID code
- Card
- Card or ID code
- Card or Windows

Identification by card requires connecting an ID device (card reader). The option **Card or Windows** allows the user to login by either card or by entering their Windows user name, password, and domain. The SafeCom G4 Server must be a member of the domain or trusted by the domain.

Default domain: Specify the domain to pre-fill the domain for users when logging into a device. If using SafeCom Mobile Pull Print, the domain must be specified, as the users are not prompted for domain when logging into a device using a smart phone. If the default domain is not specified, but the users are required to use domains, they can enter the domain with their username (domain \username).

Pre-fill domain: controls how users fill-in the domain field. In the drop-down box select:
- **Blank** (default)
- **Default domain**
- **Hide**

If users belong to different domains, **Pre-fill domain** should be left **Blank**. This means that all users need to enter their domain when they login with their Windows user name and password.

If most users belong to the same domain, select **Default domain**. **Default domain** is then filled-in for users making login easy. Users only need to use their Windows user name and password.

If all users belong to the same domain select **Hide**. Users won't be prompted for the domain when they login with their Windows user name and password. Make sure the **Default domain** is specified, otherwise **Pre-fill domain** reverts back to **Blank** when you click **Apply**.

> ⓘ The SafeCom G4 Server must be a member of the domain or trusted by the domain.

Mask ID code increases security. Use an asterisk (*) to mask the entered user code.

Print all at login is a printer setting. If selected all user documents are printed when the user logs in. Documents are printed in chronological order (oldest first). If checked this overrules the equivalent user property on the SafeCom G4 Server.

Show newest first lists and prints documents in a last-in first-out order.

MFP authentication lists the functions you can select that the SafeCom solution should authenticate. Select as many as appropriate.
- Pull Print – collect documents at any printer.
- E-mail – send scanned documents as attachments to e-mail (Enable E-mail).
- Send to Fax – send scanned documents to LAN Fax-server (Enable Send to Fax).
- Smart Scan – scan documents and store them at the Kofax SafeCom server.
- Copy – make hardcopies of scanned documents.
- Folder – send scanned documents to a network folder.
- Fax – send scanned documents through fax.
- Scanner – scan documents.
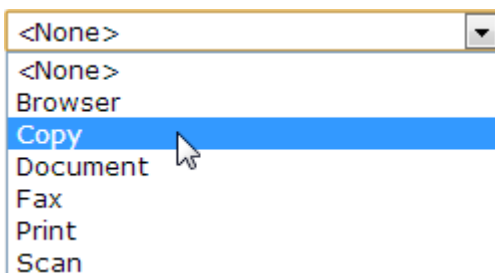
Shortcut Icon F1 and **Shortcut Icon F2** (only on MP 6002, MP 7502, MP9002, MP301, MP C305, MP4002, MP 5002, MP C3002, MP C3502, MP C4502, MP C5502) enable a configurable shortcut icon. If **<None>** is selected, no shortcut icon is displayed. If **Copy** is selected, then tapping the shortcut

icon (**F1/F2**) will bring the user straight to the MFP's copy screen, but it will start the copy process. The shortcut saves the user from first having to press the **Home** button and then tap the MFP's native **Copy** icon.

The drop down may feature items that are not supported by the device in question. It is the responsibility of the local administrator to test, that the configuration of the shortcut icon works on the particular Ricoh MFP, before end users start using the MFP. The **Shortcut** icon can also be configured through scDevUtil.exe. Refer to *SafeCom G4 Administrator's Manual* available on the Product Documentation (kofax.com) site.

Label: (only on MP 6002, MP 7502, MP9002, MP301, MP C305, MP4002, MP 5002, MP C3002, MP C3502, MP C4502, MP C5502) The text entered in the **Label** fields are presented on the touchscreen below the shortcut icons. By default, **Label** is empty and the drop down list text is used. There may be restrictions in terms of what characters can be represented as part of the label under the icon. The **Label** field can also be configured through scDevUtil.exe. Refer to *SafeCom G4 Administrator's Manual* available on the Product Documentation (kofax.com) site.

```
<CONFIGURATION>
 <NATIVE_SHORTCUTS>
  <SHORTCUT_1>
   <VALUE></VALUE>
   <LABEL></LABEL>
  </SHORTCUT_1>
  <SHORTCUT_2>
   <VALUE></VALUE>
   <LABEL></LABEL>
  </SHORTCUT_2>
 </NATIVE_SHORTCUTS>
</CONFIGURATION>
```

The reference between the value and the text in the dropdown list is as follows:

Text	Value
<None>	0
Browser	1
Copy	2
Document	3
Fax	4
Print	5
Scan	6

Post track is relevant only with SafeCom Tracking. Refer to *SafeCom G4 Administrator's Manual* available on the Product Documentation (kofax.com) site.

High speed print allows faster printing. Print speed becomes comparable to that of printing the document directly to the printer. One disadvantage is that other documents submitted through a standard TCP/IP port may print between the logged in user's print and copy jobs. Printer output does not necessarily belong to the logged in user. If directly printed documents are submitted through a SafeCom Push Port that references the same tracking device, then these documents are not printed until after the logged in user's jobs are done.

Community name: allows you to set the SNMP community name. The default value is "public". Ensure that this is set properly, as an erroneous SNMP community name will prevent SafeCom from working properly.

Drivers safeguards document fidelity in the SafeCom solution. When Pull Printing, SafeCom compares the name of the printer driver embedded in the print job with the list of driver names returned by the SafeCom device. If there is no match a question mark is displayed in the document list on the device. This way the user is warned that fidelity is in question and the document may print incorrectly.

1. Click **Get all** to retrieve a list of driver names from the SafeCom server.

2. Click **Apply**.

3. Select individual driver names on the list and click **Remove** to remove them.

4. To enter a driver name manually, click **Add driver** and then **Add**.

Connection timeout automatically logs users out after the specified amount of time. Timeout is configured in seconds with a default of 60. If there the printer requires intervention (IRQ), timeout is stopped so a user is not logged out while the issue is being resolved.

Goodbye message allows you to set a message to be displayed after each logout. The default is "Goodbye, print safely".

SafeCom Panel Lock Mode: When checked and SafeCom is the active application, users are not allowed to navigate to other applications (for example, pressing the Home button does not work). If unchecked, users are free to navigate among the device applications, but authentication when using SafeCom features (for example, Pull Print or Smart Scan) is still required.

> ℹ️ Modifying this setting requires a user login-logout, OR restarting SafeCom on the device, OR restarting the device itself.

Unlock Code: Used when **SafeCom Panel Lock Mode** is enabled. The unlock code allows users to access the device panel without logging in to SafeCom. The code locks the device panel if it is unlocked, and unlocks the device panel if it is locked. SafeCom provides feedback on the lock state through UI messages. The unlock code must meet the following criteria:
- The code must be preceded with a ***** character and followed by a **#** character.
- The code must consist of four (4) or more numbers.
- The code must be entered when SafeCom is the active application on the device.

> ℹ️ User access to device application without logging in is regulated by the External Charge Unit Management configuration option of the Ricoh device. Features selected at that configuration option can only be accessed after authentication (as such, SafeCom can provide tracking information on these features). Features not selected under External Charge Unit Management are usable without authentication, and are not tracked by SafeCom.

🛑 Do NOT select the **Printer** and **JavaTM/X** (**Extended Features** on new devices) function (Enable copy control and access control to other functions).

Log in without PIN code: Check if users do NOT need to enter a 4-digit PIN code at login. This setting applies to the device and overrules the equivalent user property on the SafeCom G4 Server. Use of PIN code is possible on devices with touch-screen or keypad.

Use **E-mail** if SafeCom handles user authentication for E-mail (**E-mail** is checked in **MFP authentication**). See Enable E-mail.

• Default From: address	:	
• Pre-fill From: field	:	Default From: address ▾
		☐ Editable
• Default To: address	:	
• Pre-fill To: field	:	User e-mail ▾
		☑ Editable
• SMTP server	:	
• Default domain	:	
• Default subject	:	
• Default body	:	
• Address Book	:	☑ Show

Use **Send to Fax** if SafeCom handles user authentication for Send to Fax (**Send to Fax** is checked in **MFP authentication**). See Enable Send to Fax.

Use **Address Book** to configure **Address Book** in **E-mail** and **Send to Fax**. See Enable SafeCom Smart Scan.

Use **Encryption** to configure the maximum length of encryption keys. See Control max length of encryption keys.

Use **Restore factory default** to reset all settings back to their default values. Click **Restore**.

Configuration web page – printers

Use the Configuration web page to configure your SafeCom Go Ricoh printer. Identification requires connecting an ID device (card reader) to the USB port at the back of the printer.

Under SafeCom Server, click Broadcast to get a complete list of servers to select from, or enter Group name, SafeCom server TCP port (default is 7500) and the SafeCom server IP address in Add server. See also Specify the SafeCom server.

> ℹ️ After you click Apply, it takes one minute before the new SafeCom Server settings take effect. Not waiting may result in a login error at the printer.

The Device name and Device model are automatically filled-in.

Device location and Contact person are important references for the SafeCom solution, so it's a good idea to fill them in.

Post track is only relevant with SafeCom Tracking. Refer to *Kofax SafeCom G4 Administrator's Manual*.

High speed print allows faster printing. Print speed becomes comparable to that of printing the document directly to the printer. One disadvantage is that other documents submitted through a standard TCP/IP port may print between the logged in user's print and copy jobs. Printer output does not necessarily belong to the logged in user. If directly printed documents are submitted through a SafeCom Push Port that references the same tracking device, then these documents are not printed until after the logged in user's jobs are done.

Drivers safeguard document fidelity in the SafeCom solution. When pull printing, SafeCom compares the name of the printer driver embedded in the print job with the list of driver names returned by the SafeCom device. If there is no match, a question mark is displayed in the document list on the device. This way the user is warned that fidelity is in question and the document may print incorrectly.

1. Click **Get all** to retrieve a list of driver names from the SafeCom server.

2. Click **Apply**.

3. Select individual driver names on the list and click **Remove** to remove them.

4. To enter a driver name manually, click **Add driver** and then **Add**.

   Use **Encryption** to configure the maximum length of encryption keys. See Control max length of encryption keys.

Encryption		▲
■ Asymmetric key max length	:	Default ▾
■ Symmetric key max length	:	Default ▾

   Use **Restore factory default** to reset all settings back to their default values. Click **Restore**.

Restore factory default	▲
	Restore

Configuration web page – MP 171, MP 201F, MP 201SPF

Use the Configuration web page to configure SafeCom Go Ricoh for the above models. Identification requires connecting an ID device (card reader) to the USB port at the back of the printer.

Under **Device**, enter specific details. Make sure to click **Apply** in the upper right corner when you have made your changes.

Device name and **Device model** are automatically filled-in. **Device location** and **Contact person** are important references for the SafeCom solution so it's a good idea to fill them in.
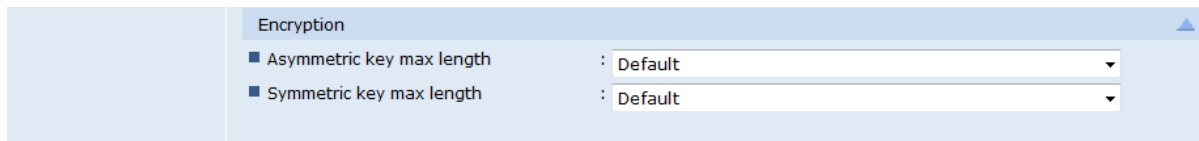
Print all at login is a printer setting. If selected, all user documents are printed when the user logs in. Documents are printed in chronological order (oldest first). If checked this overrules the equivalent user property on the SafeCom G4 Server.

MFP authentication lists the functions you can select that the SafeCom solution should authenticate. Select as many as appropriate.
- **Pull Print** – collect documents at any printer.
- **Copy** – make hard copies of scanned documents.
- **Scanner** – scan documents.

Post track is relevant only with SafeCom Tracking. Refer to *SafeCom G4 Administrator's Manual D60650* available on the Product Documentation (kofax.com) site.

High speed print allows faster printing. Print speed becomes comparable to that of printing the document directly to the printer. One disadvantage is that other documents submitted through a standard TCP/IP port may print between the logged in user's print and copy jobs. Printer output does not necessarily belong to the logged in user. If directly printed document are submitted

through a SafeCom Push Port that references the same tracking device then these documents are not printed until after the logged in user's jobs are done.

Drivers safeguard document fidelity in the SafeCom solution. When Pull Printing, SafeCom compares the name of the printer driver embedded in the print job with the list of driver names returned by the SafeCom device. If there is no match a question mark is displayed in the document list on the device. This way the user is warned that fidelity is in question and the document may print incorrectly.
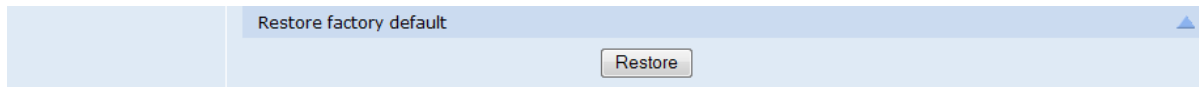
1. Click **Get all** to retrieve a list of driver names from the SafeCom server.
2. Click **Apply**.
3. Select individual driver names on the list and click **Remove** to remove them.
4. To enter a driver name manually, click **Add driver** and then **Add**.

   Timeout automatically logs users out after the specified amount of time. Timeout is configured in seconds with a default of 60. If there the printer requires intervention (IRQ), timeout is stopped so a user is not logged out while the issue is being resolved.

   Use **Encryption** to configure the maximum length of encryption keys. Refer to Control max length of encryption keys.

Use **Restore factory default** to reset all settings back to their default values. Click **Restore**.

Register web page

Use the Register web page to register the device with the SafeCom server. The printer can be used with SafeCom once it has been registered with the SafeCom server.

1. Enter the **User logon** and **PIN code** of a user with Technician or Administrator rights.

   The user must have a PIN code.

2. Click **Register**.

The device can also be registered with the SafeCom solution by:

- Using the **Add device** in **SafeCom Administrator**.
- Logging in at the device with Technician or Administrator rights.

Log web page

Use the Log web page to enable, disable and view log information.

Logging is automatically active after installing and starting the servlet and xlet. The logs are not deleted at device or servlet/xlet restart.

1. Click **Enable** to start logging.

2. Click **Disable** to stop logging (text changes on the button).

3. Click **Clear logs** to delete all logs stored on the device.

4. Click **Backup and clear logs** to back up the logs as a backup file, and clear the current logs.

Servlet and xlet logs are kept as separate files. By default, a backup is created automatically when the log file reaches the size limit (1 MB for the servlet, 5 MB for the xlet). A maximum of 10 separate log files can be created automatically; after that limit is reached, the oldest one is overwritten.

> ℹ In case of a possible problem (for example, device goes into out of order state), a ZIP file is created automatically, containing the available logs. A maximum of 3 such emergency files can be created automatically. If that limit is reached, the oldest one is overwritten.

5. Click **Show complete Log** to download all the logs files available on the device.

If the printer has a hard disk, logging data will be written to the hard disk for best performance.

If **Upload log to server** is enabled the device will upload the log to the server once an hour. The feature should *only* be enabled as per instruction by SafeCom Support. If the device is unable to upload to the server, the device will keep the log and try to upload again after yet another hour.

> ℹ️ The device will always log performance data (network latency, authentication duration of successful logins, number of **Out of order** occurrences and duration, failover and failback between G4 servers, device reboots, changes in firmware and Go versions).

Language web page

Use the Language web page to select language.
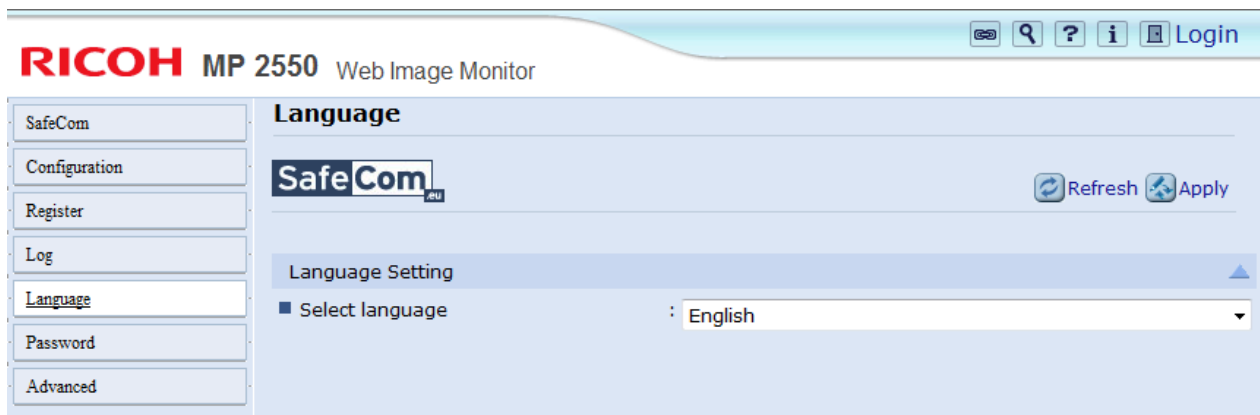
1. Select a language.
2. Click **Apply**.

The new language takes effect the next time someone logs in at the printer.

Password web page

Use the Password web page to change the password.
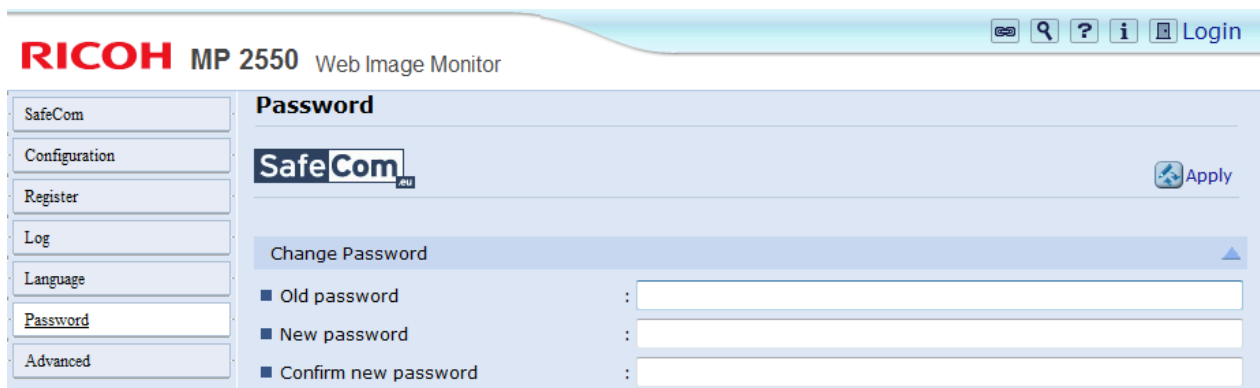
Advanced web page

Use the Advanced web page to configure parameters required for SafeCom Go Ricoh to authenticate the Kofax DigiDocFlow solution (Enable single sign-on for Kofax DigiDocFlow), NSi

AutoStore (Enable single sign-on for NSi AutoStore), Extended Feature Shortcut (Enable Extended Feature Shortcut), or AAA (Enable AAA).

SafeCom Go Ricoh – How to

The following subsections contain step-by-step instructions for some common administrator tasks.

Get the SafeCom Go Ricoh software

The SafeCom Go Ricoh software files (*.b87) and SafeCom Go Ricoh uninstall files (*.uin) can be downloaded using the SafeCom Administrator function Check for updates.

Alternatively, a software package can be downloaded:

1. Download the safecom_go_ricoh_xxx.exe file from the link supplied to you.
2. Double-click the safecom_go_ricoh_xxx.exe file.
3. Click **Next**.
4. Select the destination folder. Click **Next**.

    Normally, the destination folder is at `C:\Program Files\SafeCom\SafeComG4\device_software`.
5. Click **Install**.
6. Click **Finish**. To install software through Ricoh's deployment tool, **RiDeploy**, use the files located in the Ricoh type specific subfolders, /ricoh_deploy_files_type/.

Specify the SafeCom server

1. Open the Configuration web page (Configuration web page).

2. To exclude broadcast results from SafeCom servers that do not belong to a particular SafeCom group in a multiserver solution, enter the **Group name**.

3. Click **Broadcast**.

It takes approx. 5 seconds for the broadcast results to populate the **SafeCom server IP address** list. If the SafeCom server has multiple IP addresses, there will be an entry for each. If the SafeCom server is clustered, you must ensure that the entry only matches the IP address of the virtual server and not the nodes. In a multiserver solution, click **Move up** and **Move down** to prioritize the order in which the servers are contacted in case the first one on the list becomes unavailable. If the device is added through SafeCom Administrator, the list of SafeCom servers will include the list of prioritized failover servers. For additional information about failover servers, refer to *SafeCom G4 Administrator's Manual D60650* available on the Product Documentation (kofax.com) site. If broadcasting fails, you may have to directly enter the IP address in **Add server** and click **Add**.

4. Click **Apply**.

ⓘ After you click **Apply**, it takes a minute before the new SafeCom Server settings take effect. Wait; otherwise there may be a login error at the printer.

Resend configuration

If a device added in the SafeCom Administrator is not configured correctly, or if the device must be reconfigured to a different server, it is possible to resend configuration details (Server address and Group name) to the device.

1. Browse to **Devices** in the SafeCom Administrator.

2. Right-click the device and click **Resend configuration**.

> ℹ The Resend configuration functionality does not work with devices that are SafeCom enabled through the device server.

The configuration details are now sent to the device and the configuration is successful when **Server is reconfigured** appears.

Register device

1. Open the Register web page.
2. Enter the user logon and PIN code of a user with technician or administrator rights.
   The user must have a PIN code.
3. Click **Register**.
   Once the device is registered it appears in the SafeCom Administrator. The device can also be registered with the SafeCom solution when:
   - Using the Add device function in the SafeCom Administrator.
   - Logging in at the device if the user has technician or administrator rights.

Set password to prevent unauthorized access

1. Open the Password web page (Password web page).
2. Enter the old password and the new password twice.
   The password is 8 characters maximum.
3. Click **Apply**.

> ℹ Make sure to store the password in a secure place. If you forget the password, you need to uninstall SafeCom Go Ricoh.

Check SNMP settings

If SNMP v1/v2 is disabled, SafeCom Go Ricoh is unable to obtain the correct MAC address of the printer and will report the MAC address 111badadd111 instead. Follow these steps to check and correct the SNMP settings.

1. Open the printer's web page by entering its IP address in a web browser.
2. Click **Login** and supply the user name (admin) and password (blank).
3. Click **Configuration** on the menu.
4. Click **Network** on the menu.
5. Enable **SNMPv1/v2 Function**.
6. Click **Apply**.

Select user identification – user code or card

Identification by card requires the installation of a SafeCom ID device (card reader) and possibly a SafeCom Go Ricoh SD ID Kit.

> ℹ️ ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

1. Open the Configuration web page (Configuration web page).
2. Change **User identification** to **Card, Card or User code** or **Card or Windows**.
3. Click **Apply**.

Login with Windows without specifying the domain

It is possible to log in by entering your Windows user name, password, and domain. If all users belong to the same domain, you can avoid prompting users to enter the domain at the device.

1. Open the Configuration web page (Configuration web page).
2. Specify a default domain.
3. Change **Pre-fill domain** to **Hide**.
4. Click **Apply**.

How to make SafeCom stay always on top

1. On the device, press the **User Tools** button (<>/123).
2. Tap **System Settings** and then tap the **General Features** tab.
3. Tap **Function Priority** and then tap the **Extended Feature** tab. Tap **SafeCom Go**, then tap **OK**.

   > ℹ️ On older devices (pre-Java 11.x), the **Extended Feature** tab is called **JavaTM/X**.

4. Tap **Print Priority** and then tap the **Display Mode** tab. Tap **OK**.
5. Tap **Exit**.
6. Tap **Extended Feature Settings** and then tap **Extended Feature Settings**.
7. Tap the **Startup Setting** tab. Tap **Priority** next to SafeCom Go if SafeCom is not selected under **Extended Feature Name**.
8. Tap **Exit** and then **Exit** to leave **User tools**.

Enable copy control and access control to other functions

To enable copy control and access control to other functions, on all devices (except types C):

- Have your Ricoh technician bring the Ricoh device into SP mode.
- SP-5401 Access Control:
- Default Document ACL (103) set to 3
- Commit changes by pressing the # key
- SDK Certification Device (230) set to 00000001
- Commit changes by pressing the # key
- SP-5113 Optional Counter Type
- External Optional Counter Type (1) set to 1:Expansion Device 1
- Commit changes by pressing the OK button. Then press Exit and Exit.

See also Control user access rights.

1. On the printer press the **User Tools** button (<>/123).
2. On the touch-screen, tap **System Settings** and then tap **Administrator Tools** tab.
3. Tap **Enhanced External charge Unit Management** and select the functions you want to have access control for.

   The relevant functions include **Copier**, **Document Server**, **Facsimile** and **Scanner**). Do NOT select the **Printer** and **JavaTM/X** (**Extended Features** on new devices) function.
4. Press **OK** to save changes.
5. Tap **Exit** and **Exit** to leave **User Tools**.
6. Open the Configuration web page (Configuration web page).
7. Check **Copy** in **MFP authentication**. Please check the additional functions that are controlled by SafeCom.
8. Make your selections in the **E-mail** (Enable E-mail) and **Send to Fax** (Enable Send to Fax) sections.
9. Click **Apply**.
10. Restart the device.

Enable E-mail

SafeCom Go Ricoh comes with its own intuitive E-mail function (E-mail).

1. Open the Configuration web page (Configuration web page).
2. Check **E-mail** in **MFP authentication**.
3. Make your selections in the **E-mail** section.
4. Click **Apply**.

By default, the **From:** field is not **Editable** and the **To:** field is **Editable**. By default, both fields are pre-filled with the **User e-mail**.

Default From: address: Can be pre-filled with User e-mail, Blank or Default From: address.

An e-mail sent with pre-filled **User e-mail** of the user John Smith with the e-mail address js@safecom.eu will appear as:

```
From: js@safecom.eu
```

If the user does not have an e-mail address, the **Default From: address** is used. If this is not configured then no_reply@safecom.invalid is used.

Default To: address: This field can be pre-filled with **User e-mail**, **Blank** or **Default To: address**. The **CC:** and **BCC:** fields are only editable if the **To:** field is editable.

SMTP Server: This must be configured with the address (IP address or hostname) of the mail system.

Default domain is the optional e-mail domain that is appended if the @ character is <u>not</u> found in the text entered in the **To:**, **CC:** and **BCC:** fields. Example: The software will automatically expand 'js' to 'js@safecom.eu' if the specified default domain is safecom.eu.

Default subject is the optional text that appears as the subject of the e-mail.

Default body is the optional text that appears in the body of the e-mail.

Address Book buttons are available in the E-mail dialog on the services touch-screen if you check **Show** (E-mail).

Enable Send to Fax

SafeCom Go Ricoh comes with its own intuitive Send to Fax function (Send to Fax).

> ℹ The SafeCom Go Send to Fax function is a LAN Fax-server solution. If you want to use the built-in phone line solution, then you must disable Counting control for the Facsimile function (Enable copy control and access control to other functions).

1. Open the Configuration web page (Configuration web page).
2. Check **Send to Fax** in **MFP authentication**.
3. Make your selections in the **Send to Fax** section.
4. Click **Apply**.

Send to Fax		▲
■ Default From: address	:	no_reply@safecom.invalid
■ Pre-fill From: field	:	User e-mail ▼
		☐ Editable
■ Scan format	:	TIFF ▼
■ Default domain	:	
■ Default subject	:	
■ Default body	:	
■ Address Book	:	☐ Show

By default, the **From:** field is not **Editable** and can be pre-filled with **User e-mail**, **Blank**, or **Default From: address**.

A fax sent with pre-filled **User e-mail** of the user John Smith with the e-mail address js@safecom.eu will appear as:

```
From: js@safecom.eu
```

Default From: address: Use if the user does not have an e-mail address. If this is not configured then no_reply@safecom.invalid is used.

Scan format specifies whether scanning is in **TIFF**, **PDF**, or **JPEG** format.

Default domain is the optional fax domain that is appended if no @ character is found in the text entered in the **To:** field. For example, the software will automatically expand the phone number '12345667' to '12345667@safecom.eu' if the specified default domain is safecom.eu.

Default subject is for optional fax subject text.

Default body is for optional text for the body of the fax.

Address Book buttons are shown on the device's touch screen in the Send to Fax. Click **Show** (E-mail).
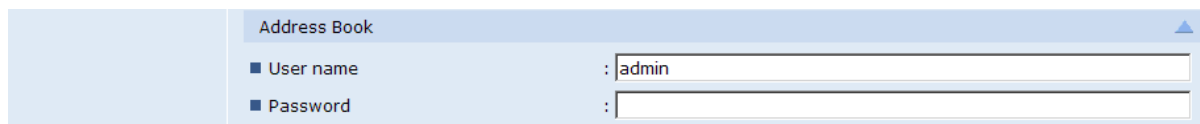
Enable SafeCom Smart Scan

The SafeCom Smart Scan feature allows users to scan a document and then manage or download the scanned files from either the SafeCom Web Interface (*SafeCom G4 Web Interface Administrator's Manual D60651*) or from the SafeCom Move (*SafeCom G4 Administrator's Manual D60650*) available on the Product Documentation (kofax.com) site.

1. Open the Configuration web page (Configuration web page).
2. Scroll to the **Device** section and check **Smart Scan**.
3. Click **Apply**.

Enable Address Book

SafeCom Go Ricoh can use the Ricoh Address Book with E-mail (E-mail) and Send to Fax (Send to Fax).

1. Open the Configuration web page (Configuration web page).
2. Scroll to the **Address Book** section at the bottom of the page.
3. Enter the user name and password of the administrator of the Ricoh MFP.
4. Click **Apply**.

Address Book		
■ User name	:	admin
■ Password	:	

ⓘ Refer to the documentation that came with the Ricoh MFP in order to learn how to build and maintain the Address Book.

Control max length of encryption keys

Skip this section if you use the SafeCom G2 server.

1. Open the Configuration web page (Configuration web page).
2. Scroll to the **Encryption** section at the bottom of the page.
3. **Asymmetric key max length** can be: **Default**, **512**, **1024**, or **2048**. **Symmetric key max length** can be: **Default**, **128** or **256**.
4. Click **Apply**.

Select **Default** to leave it to the device to decide if it has sufficient processing power and memory to comply with the length of the encryption keys that has been specified on the **Encryption tab** in the **Server properties** dialog of the SafeCom G4 Server.

SafeCom control data to and from the device is always encrypted. Pull printed documents are sent encrypted to the device only if **Encryption** is checked in the **Device properties** dialog and if the user has **Encrypt documents** checked on the **Settings** tab in the **User properties** dialog. Otherwise, print data is NOT encrypted.

Control user access rights

When using SafeCom G3 Server version S82 070.440*03 or newer, you can control users' access rights to specific features through SafeCom Administrator, refer to *SafeCom G4 Administrator's Manual D60650* available on the Product Documentation (kofax.com) site. You can control access rights to the following features:

- Copy
- E-mail
- Scan
- Fax
- Print all

Enable single sign-on for Kofax DigiDocFlow

1. Open the Advanced web page (Advanced web page).
2. Enter **Computer IP address** and **Port** (default 21) of the computer hosting the Kofax DigiDocFlow solution.
3. Enter **User name** and **Password** required to access the Kofax DigiDocFlow solution.
   The **External authentication** section is only used for NSi AutoStore (Enable single sign-on for Kofax DigiDocFlow). Leave **Enable** unchecked.
4. Click **Apply**.

Enable single sign-on for NSi AutoStore

- From SafeCom, obtain the file scNotifyExtAuth.dll.
- From NSi AutoStore, obtain the client package that contains ASEQTC.exe.

ⓘ Both SafeCom server and AutoStore MUST be in the same domain. SafeCom service MUST be started by a user with remote access rights on the AutoStore server.

Enable single sign-on on each SafeCom server

These steps must be repeated on each SafeCom server:

1. Run the AS_Equitrac_Client_to_be_installed_on_Equitrac_Server.exe as administrator and enter the IP address of the AutoStore Server.
   After installation, you should see a new service called ASEQAT.
2. Stop the SafeCom Service and copy the scNotifyExtAuth.dll into the SafeCom installation folder.
3. Right-click **SafeCom Service** and click **Properties**.
4. Click the **Log on** tab and click **This account**. Enter the name and password of an account that has remote access rights on the AutoStore server.
5. Click **OK**.
6. Restart the SafeCom Service.

   ⓘ The SafeCom Service loads the IP address of the AutoStore server when it is started. This implies that a change of the AutoStore server's IP address should be followed by a restart of the SafeCom Service.

Enable single sign-on on the Ricoh device

These steps need to be performed on the Ricoh device:

1. Increase the Heap Size on the Ricoh device to about 24 MB, and configure the diprint timeout (Configure the Diprint Timeout value on the Ricoh device).
2. Open the Advanced web page (Advanced web page).
3. Check **Enable** under **External authentication**. Leave all other fields at their default.
4. Click **Apply**.

Enable Extended Feature Shortcut

To add a shortcut to the SafeCom main screen that takes users to another application, add the "Extended Feature Shortcut".

---

[1] The client package is generic in nature, but is most likely known as "AutoStore EquiTrac Client".
[2] As of June 2021, no testing has been performed with trusted domains.

ℹ️ Not available on all Ricoh models.

1. Open the Advanced web page (Advanced web page).
2. Check **Enable** under **Extended Feature Shortcut**.
3. Enter the software ID number in **Product ID**.
4. Enter the name you want displayed on the SafeCom main screen in **Label**.
5. Click **Apply**.

Enable AAA

To allow for single sign on to various AAA-using applications, enable Ricoh AAA support.

ℹ️ Applications using AAA often require additional configuration steps. Check the relevant documentation of the application in question.

1. Open the Advanced web page (Advanced web page).
2. Check **Enable** under **Ricoh AAA**.
3. Click **Apply**.
4. Check if AAA is running on the device.

Using Smart Operating Panel

For the requirements of the Smart Operating Panel, see Requirements.

Restore factory default

1. Open the Configuration web page (Configuration web page).
2. Click **Restore**.

Configure timeouts

1. Configure the System Auto Reset Timer of the device.
2. Configure the SafeCom timeout value through the SafeCom configuration page of the device (Configuration web page).
3. Set SafeCom to be the **Function Priority** application on the device or the SOP panel.

   This allows the System Auto Reset Timer to take the user to the SafeCom screen.

   Using the above configuration steps, idle users on the SafeCom screen are logged out once the SafeCom timeout elapses. Idle users on native application screens (for example, the Copy screen) are taken to the SafeCom screen once the System Auto Reset Timer elapses. At that point, the SafeCom timer (re)starts, and the user is logged out if remaining idle until the timer elapses.

   If SafeCom is not configured as the Function Priority application on either the device or the SOP panel, make sure you set the System Auto Reset Timer to a higher value than the SafeCom timer. This ensures that when the user leaves the device with the SafeCom screen displayed, SafeCom will time out before the device navigates to a different screen.

Determine the version

The version of the SafeCom Go Ricoh software can be determined from the Information web page.

Open the Information web page (Information web page).
The version can also be seen in the **Device properties** dialog in SafeCom Administrator.

Uninstall SafeCom Go Ricoh

> ⓘ Using this uninstallation method is the recommended safe way of removing the application to ensure removal of all relevant components.

1. Make sure the printer is powered on and ready.
2. Start SafeCom Administrator and log in to the server.
3. Right-click the Ricoh device and click **Update software**.
4. Browse to the SafeCom Go Ricoh uninstall file.
   Example: 090xxx.uin
5. Click **Send** to send the SafeCom Go Ricoh Software (*.uin) file to the device. If file is not present you need to get the file first (Get the SafeCom Go Ricoh software).
   After uninstallation, the device restarts.

> ⓘ If the device gets stuck with the message "Please wait", then restart it again.

All printing through SafeCom

Follow the steps below to restrict printing to SafeCom.
1. Open the printer's web page by entering its IP address in a web browser.
2. Click **Login** and supply the user name (admin) and password (blank).
3. Click **Configuration** on the menu.
4. Under **Security**, click **Access Control**.
5. Enter the **IP Address** of the SafeCom server as both the start and end point of the Access Control Range.
6. Click **OK**.
   You may also need to disable selected network printing protocols, such as the Internet Printing Protocol (IPP).
7. Under **Network**, click the protocols you want to disable.

Install SafeCom Go Ricoh through web page

Before proceeding, check that the device_software folder (Get the SafeCom Go Ricoh software) contains the Ricoh type-specific subfolders, /ricoh_deploy_files_type_{?}.

Install file types C, F, I, J, L, N

1. Open a web browser and enter the printer's address.

   JavaScript (Active Scripting) must be enabled.
2. Click **Login** and enter **Login User Name** (admin) and **Login Password** (by default there is no password) and then click **Login**.
3. Click **Configuration** on the left menu.
4. Under **Extended Feature Settings**, click **Install**.
5. Select **Local File** and click **Browse** to locate the Ricoh type specific subfolders, / ricoh_deploy_files_type_? and select the nnnxxx_servlet.zip file. Click **Open**.
6. Click **Display Extended Feature List**.
7. Leave **Install to** as is.
8. In **Auto Start**, click **On**.
9. On the **Extended Feature List**, click **RicohServlet**.
10. Click **Install**.
11. On the Confirm web page, click **OK**.

Install SafeCom Go (SafeCom Go Xlet):
12. Select **Local File** and click **Browse** to locate the Ricoh type specific subfolders, / ricoh_deploy_files_type_? and select the nnnxxx_xlet.zip file. Click **Open**.
13. Click **Display Extended Feature List**.
14. Leave **Install to** as is.
15. In **Auto Start**, click **On**.
16. On the **Extended Feature List**, click **SafeCom Go**.
17. Click **Install**.
18. On the Confirm web page, click **OK**.
19. Restart the printer.

Install file types H, K, O

1. Open a web browser and enter the printer's address.

   JavaScript (Active Scripting) must be enabled.
2. Click **Login** and enter **Login User Name** (admin) and **Login Password** (by default, there is no password) and then click **Login**.
3. Click **Configuration** on the left menu.
4. Under **Extended Feature Settings**, click **Install**.
5. Select **Local File** and click **Browse** to locate the Ricoh type specific subfolders, / ricoh_deploy_files_type_h and select the 080xxx_servlet.zip file. Click **Open**.
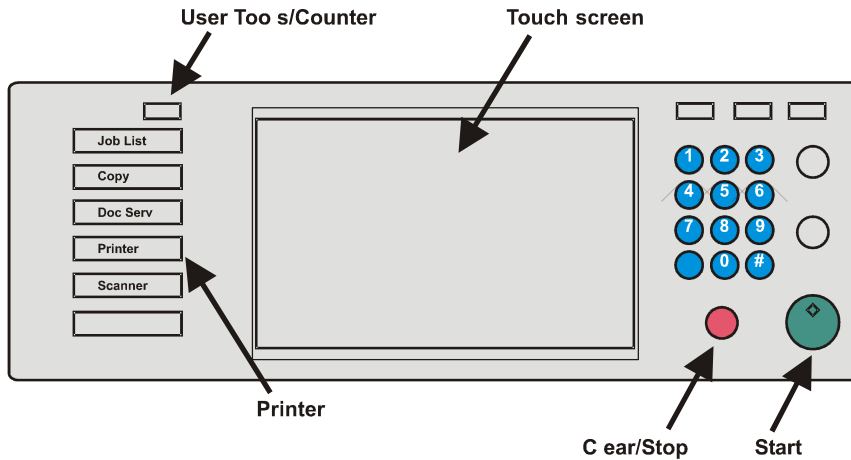
6. Click **Display Extended Feature List**.
7. In **Install to**, select **SD Card Slot 1**, where 1 is the slot with the VM Card.
8. In **Auto Start**, click **On**.
9. On the **Extended Feature List**, click **RicohServlet**.
10. Click **Install**.
11. On the Confirm web page, click **OK**.
12. Restart the printer.

Chapter 3

Using SafeCom Go Ricoh

Ricoh Aficio MFPs

The control panel is as follows:

Login

The recommended login sequences are described below.

Log in with card

1. Press the **Other Function** button on the device.
   This opens the SafeCom login screen "Use card to log in".
2. Use the card reader.
3. Tap the **Pull Print** or **E-mail** icon or press the **Copy** button.

Log in with card and PIN code

1. Press the **Other Function** button on the device.
   This opens the SafeCom login screen "Use card to log in".
2. Use the card reader.
3. Enter the PIN code on the keypad or touch-screen. Tap **OK**.

4. Tap the **Pull Print** or **E-mail** icon or press the **Copy** button.

Log in with user code

1. Press the **Other Function** button on the device.
   This opens the SafeCom login screen "Touch screen to login".
2. Tap the screen.
3. Enter the user code on the touch-screen. Tap **OK**.
4. Tap the **Pull Print** or **E-mail** icon or press the **Copy** button.

Log in with user code and PIN code

1. Press the **Other Function** button on the device.
   This opens the SafeCom login screen "Touch screen to login".
2. Tap the screen.
3. Tap **User code** and enter the user code on the touch-screen. Tap **OK**.
4. Tap **PIN code** and enter the PIN code on the keypad or touch-screen. Tap **OK**.
5. Tap the **Pull Print** or **E-mail** icon or press the **Copy** button.

Log in with Windows

If User identification (Select user identification – user code or card) is Card or Windows, it is possible to log in by either using your card or entering your Windows login credentials.

1. Press the **Other Function** button on the device.
   This opens the SafeCom login screen "Touch screen to login".
2. Tap the screen.
3. Tap **User name** and enter the user name on the touch-screen. Tap **OK**.
4. Tap **Password** and enter the password on the touch-screen. Tap **OK**.

   > ⓘ The **User name** and **Password** fields cannot be empty.

5. Tap **Domain** and enter the domain on the touch-screen. Tap **OK**.
   The solution can be configured to NOT prompt for the domain (Login with Windows without specifying the domain).
6. Tap **Login**.

Pull print
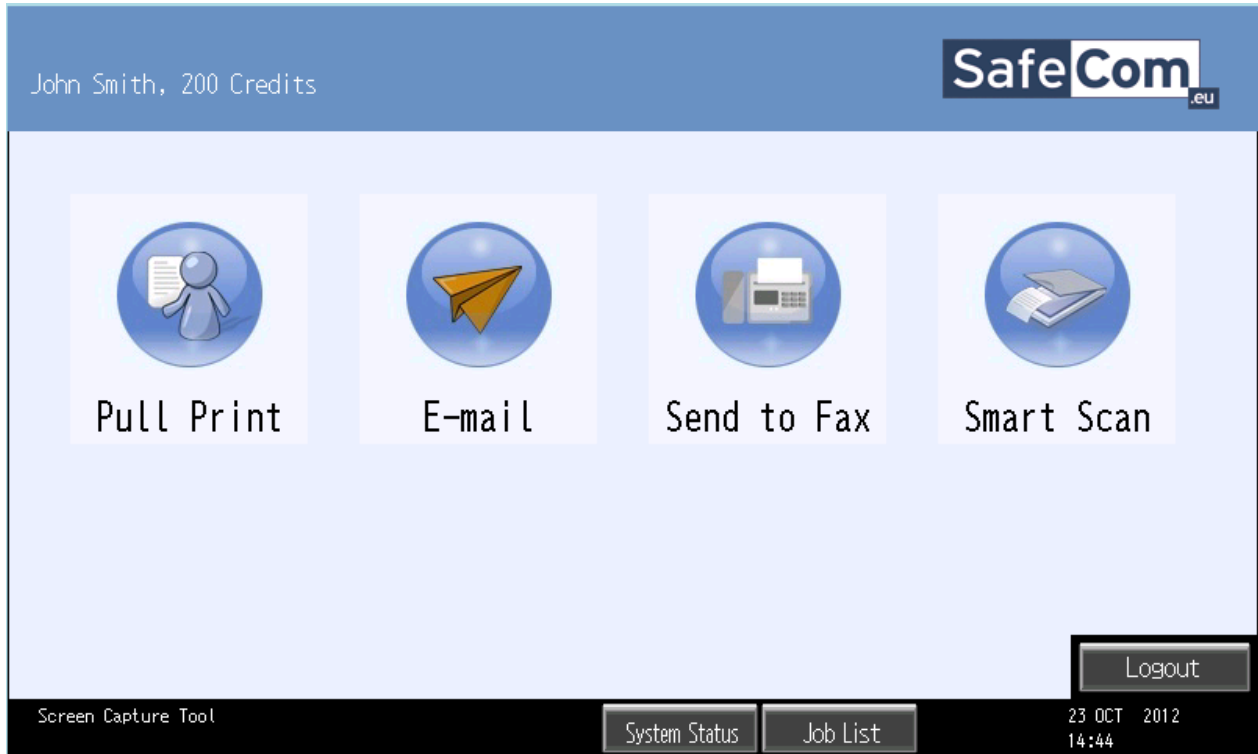
Tap **Pull Print** to access the **Document list** that allows you to print individual documents. Documents are listed chronologically with the newest at the top. If **Print all at login** is checked, documents pending collection are printed first.
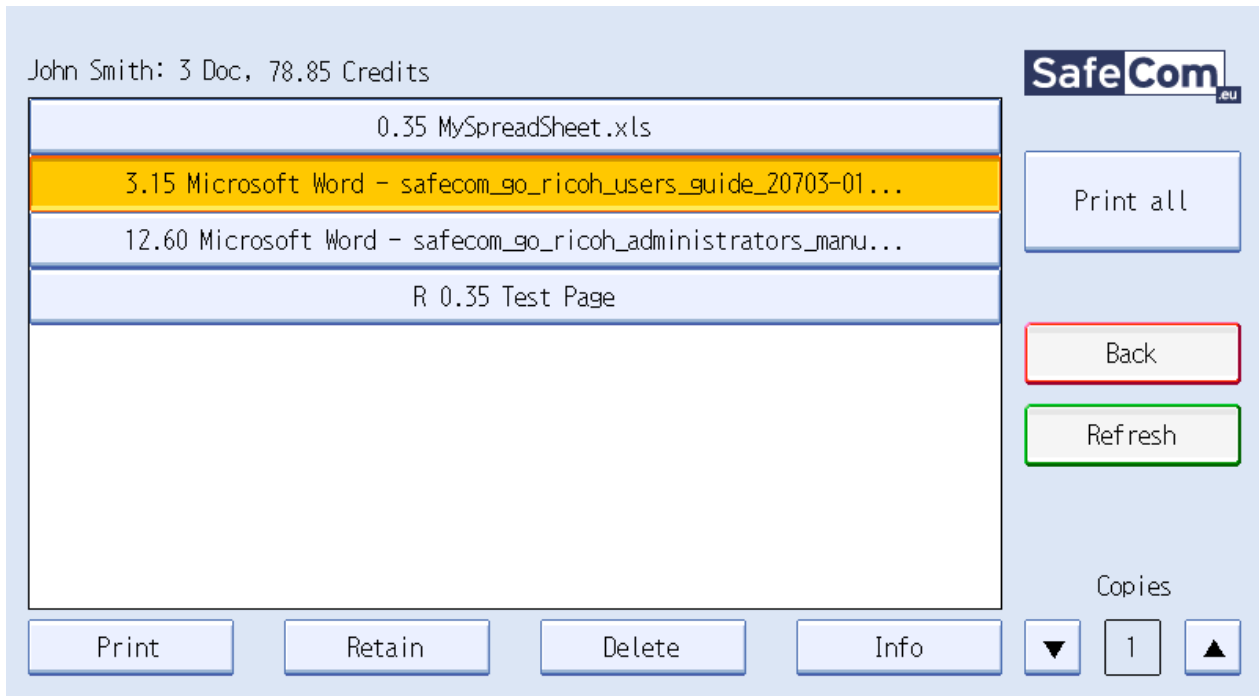
In the document list, a document with a preceding R shows the document is retained. A delegated document will have a preceding D. Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding G. In the figure, 0.35 is the cost of the document.

- Tap **Print all** to print all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
- Tap **Delete** to delete the selected documents.
- Tap **Info** for information about the selected documents, including cost, driver name, use of color and duplex.
- Tap **Refresh** to update the list of documents with pending documents that have finished spooling after the user logged in.
- Use the physical keypad or the up and down buttons to enter the number of copies you want of the selected documents. Press the red **Clear/Stop** button to reset copies to 1.

Copy

After login (Login), press the **Copy** button and then the **Start** button to copy the documents placed in the automatic document feeder (ADF).

E-mail
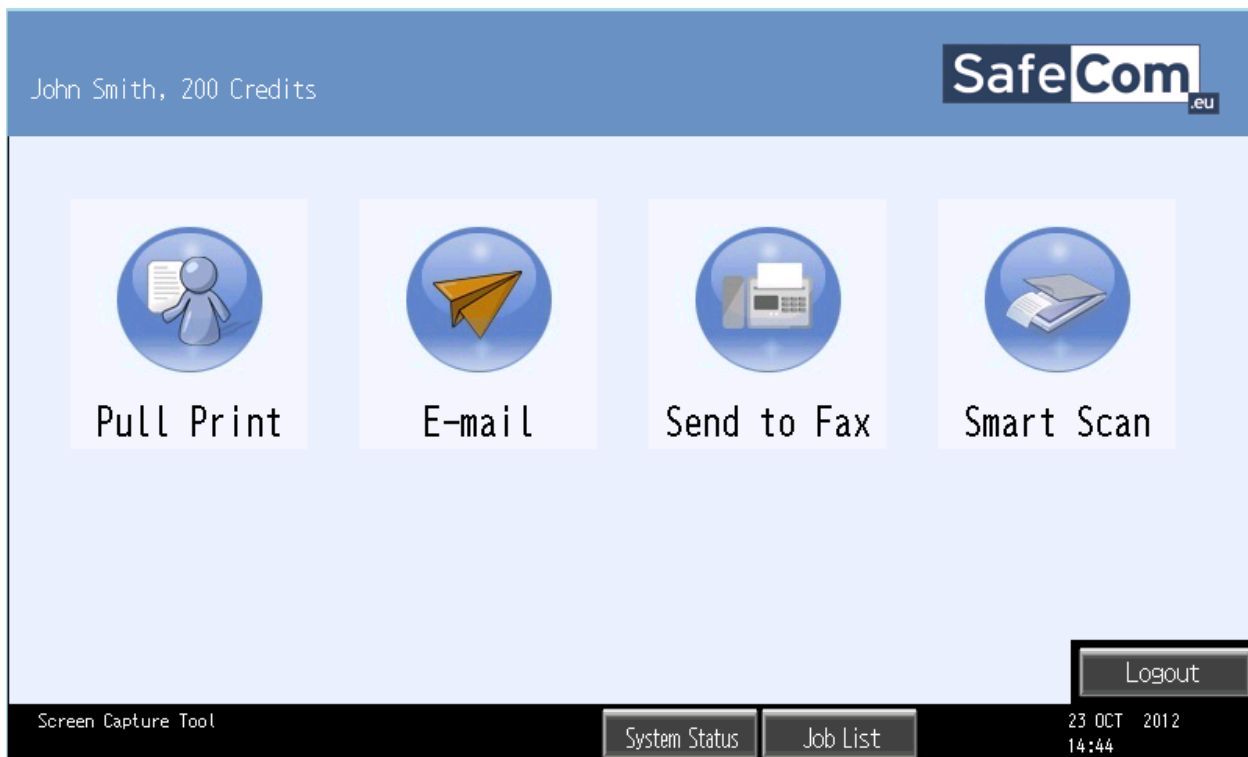
Tap the **E-mail** icon.

The **To:** field can be pre-filled with the User e-mail, Blank or Default To: address.

The From: field can be pre-filled with User e-mail, Device name, Blank or Default From: address. See Enable E-mail.

To enter an email address, tap the field and enter the address using the touch-screen, keypad, or **Address Book** button to the right of the field (Smart Scan).

Tap **Send** to send the document.
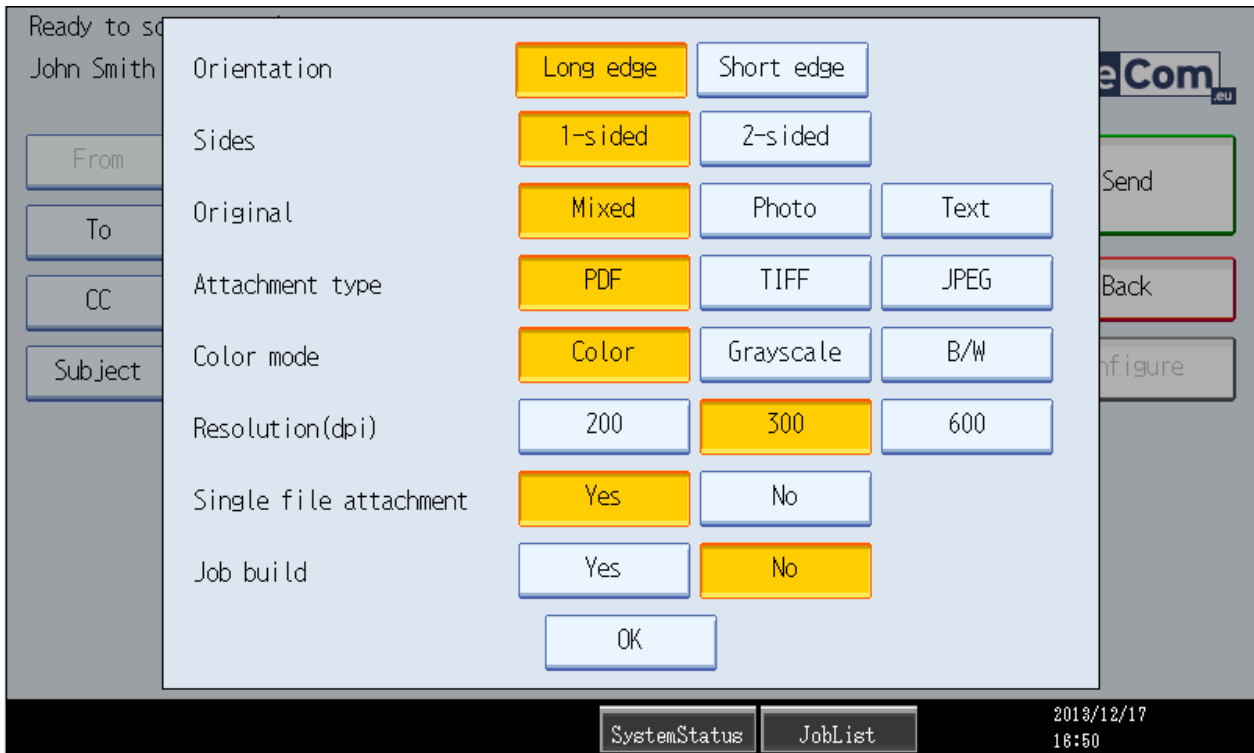
Tap **Back** to go back to the main screen.

Tap **Configure** to select scan properties.

Scan properties include:

- Orientation [Long edge, Short edge]
- Sides [1-sided, 2-sided]
- Original [Mixed, Photo, Text]
- Attachment [PDF | TIFF | JPEG]
- Color mode [Color, Grayscale, B/W]
- Resolution (dpi) [200, 300, 600], default is 200 dpi (can be configured on the Configuration web page (Configuration web page)
- Single file attachment [Yes, No]

- Job Build [Yes, No] – allows multiple documents to be scanned to a single file. By default, Job Build is turned off.

Tap **OK** to return to sending e-mail.

Send to Fax

Tap the **Send to Fax** icon. In the To: and CC: field enter the receiver's fax number.

The From: field can be pre-filled with User e-mail, Device name, Blank or Default From: address. See Enable Send to Fax.

Tap **To**, **CC**, and **Subject** and use the touch-screen keypad or the **Address Book** to the right of the field (Smart Scan) to enter fax recipients and subject.

Tap **Send** to scan and fax the document.

Tap **Back** to return to the main screen.

Smart Scan

Put the document in the document feeder and tap the **Smart Scan** icon.
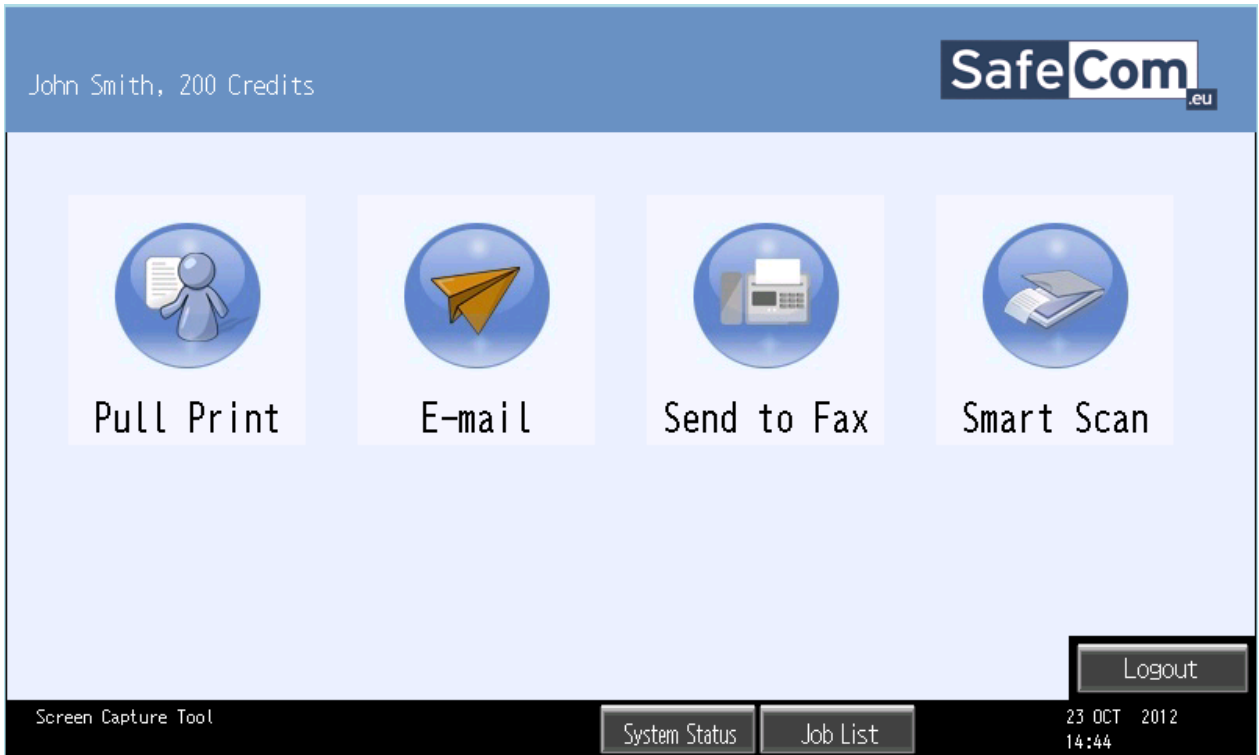
Enter a prefix for the document. The document name is the prefix followed by a timestamp. If a scanned file entails more than one page, the file name is also followed by a number that increment by 1 for each new file (for example, agenda20121010152801_0).

The default file name is the timestamp.

Tap **Configure** to make changes to the scan properties and then tap **OK**.
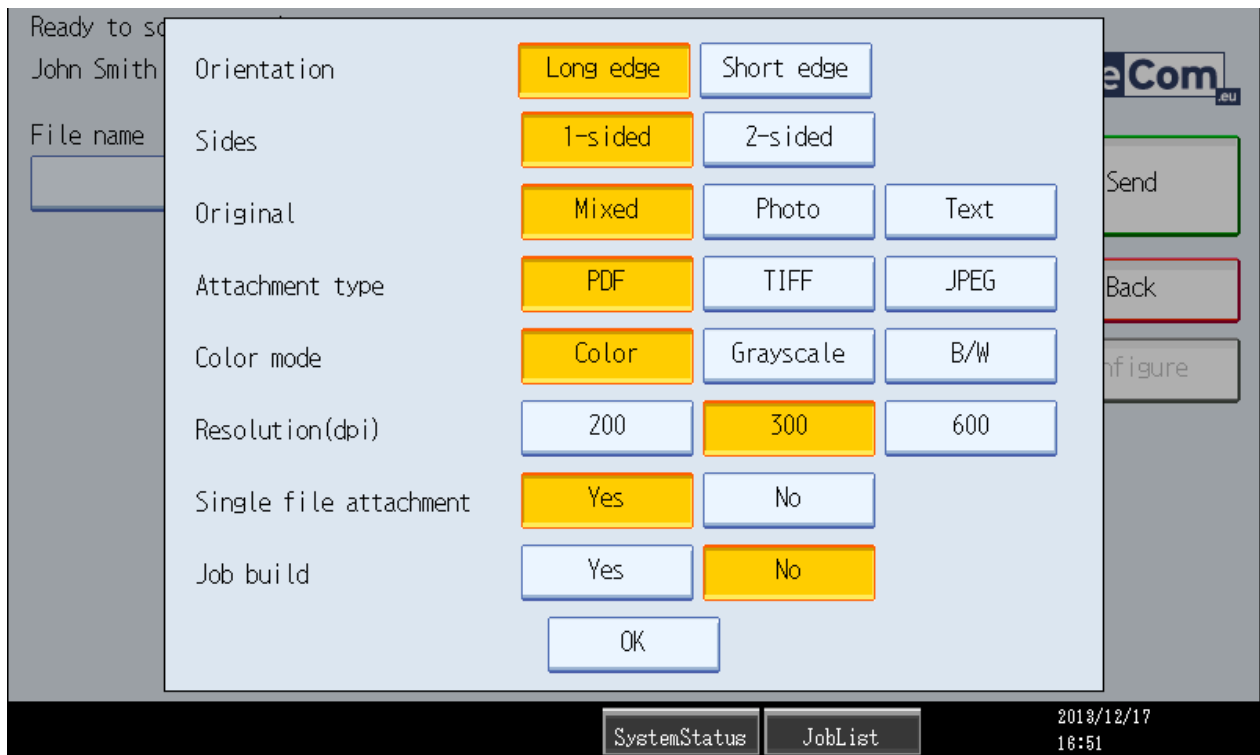
Scan properties include:
- Orientation [Long edge, Short edge]
- Sides [1-sided, 2-sided]
- Original [Mixed, Photo, Text]
- Attachment [PDF | TIFF | JPEG]
- Color mode [Color, Grayscale, B/W]
- Resolution (dpi) [200, 300, 600], default is 200 (can be configured on the Configuration web page (Configuration web page)
- Single file attachment [Yes, No]
- Job Build [Yes, No] – allows multiple documents to be scanned to a single file. By default, Job Build is turned off.

Tap **Scan** to scan the document.

Tap **Back** to return to the main screen.

Now the scanned files are available for download in either the SafeCom Web Interface or SafeCom Move.

Address Book

Enable the Ricoh MFP's Address Book (Enable SafeCom Smart Scan) and use it for easy selection of **E-mail** (E-mail) and **Send to Fax** (Send to Fax) recipients.

Tap the **Address Book** button in **E-mail** or **Send to Fax**. In **Find**, enter the text to perform a case insensitive search for recipients. Tap **OK**.
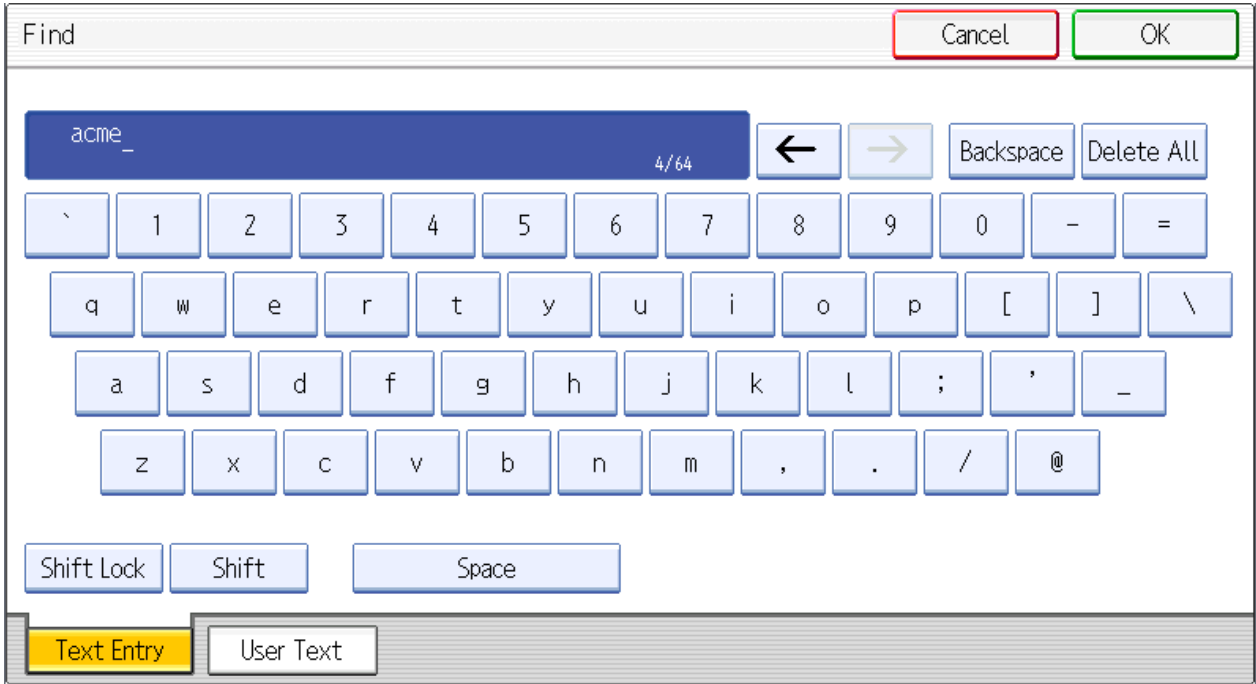
E-mail recipients look like this:

Send to Fax recipients look like this:
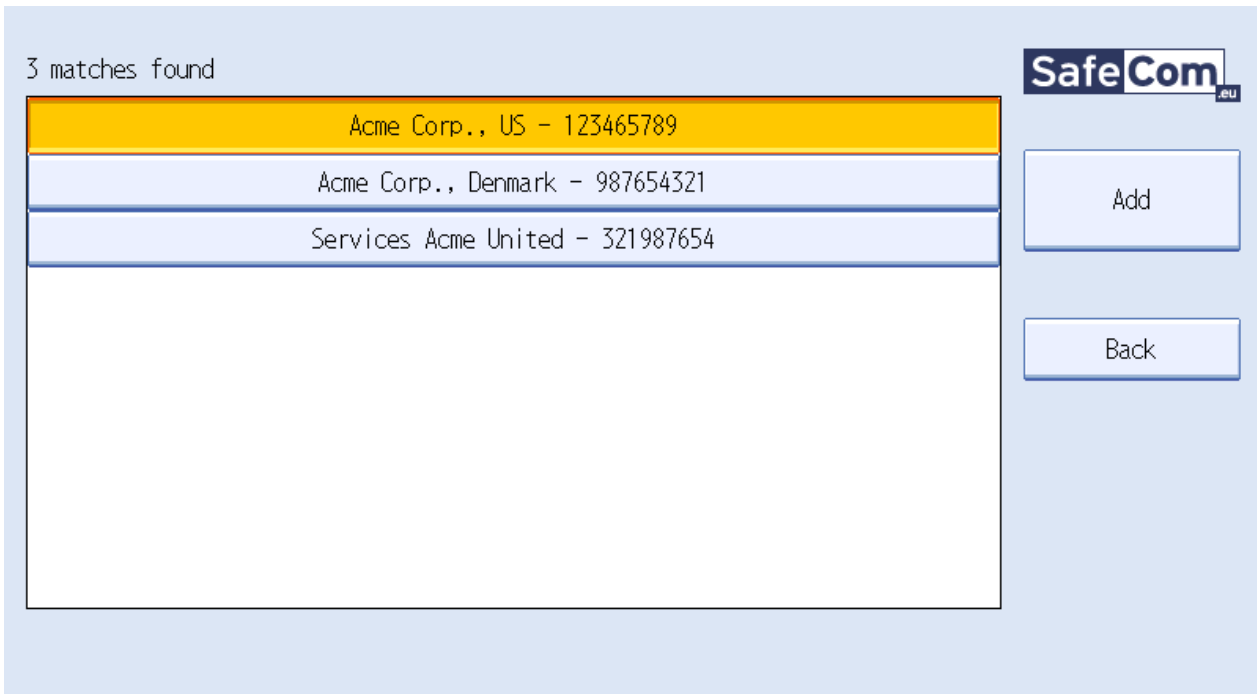
Select the recipients and tap **Add**.

Logout

There is a configurable timeout with a default time of 60 seconds. Users are logged out if the device is idle for this period of time.

To logout actively:

- Tap **Logout** in the list of icons.
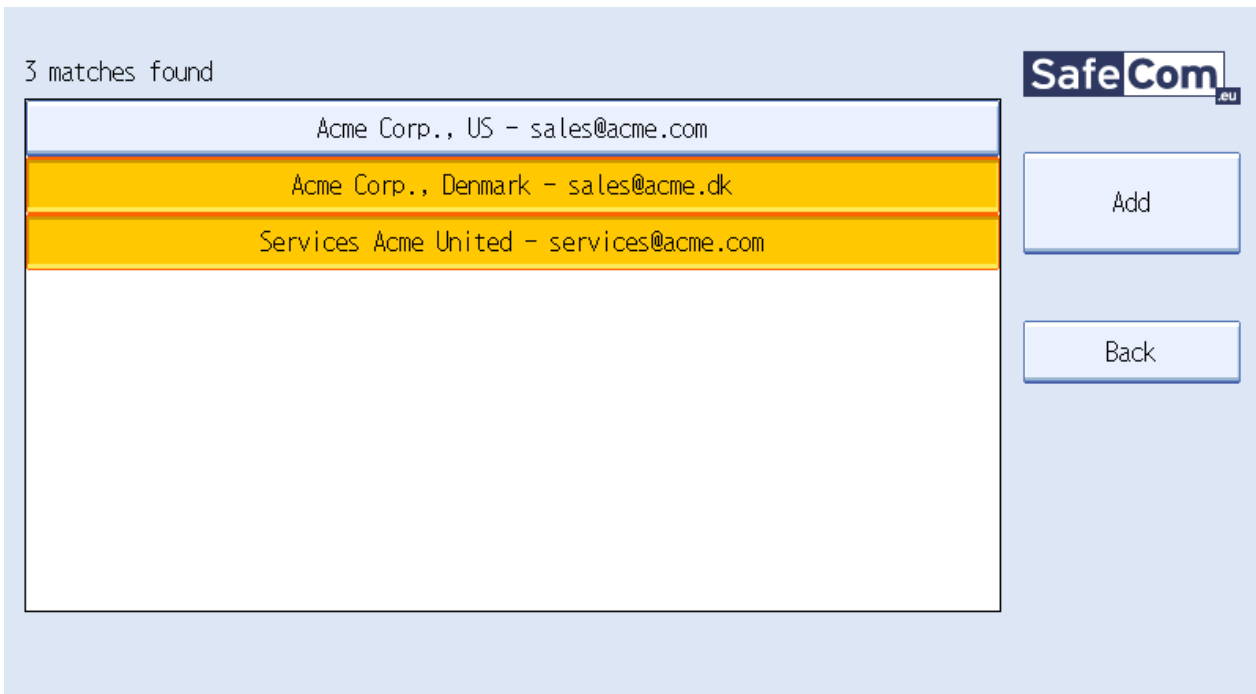- Use card again (if a card reader is connected and you logged in by card).

Register card at device

There are two ways the user can register a card at the device:

- Register card with Windows logon: User must have a network logon and the **User identification** (Configuration web page) must include card.
- Register card with PUK code: PUK code must be supplied to the user in advance, typically through e-mail.

Register card with Windows logon

1. Use the card reader.
   - If there are any available PUK codes on the system, tap **Cancel** in the **Please enter PUK** dialog.

The **Login to register card** dialog appears.

- If there are NO available PUK codes, the user gets the **Login to register card** dialog. To abort the registration of the card, tap **Cancel** in this dialog.

2. Tap **User name** and enter the user name on the touch-screen. Tap **OK**.
3. Tap **Password** and enter the password on the touch-screen. Tap **OK**.

> ℹ The **User name** and **Password** fields cannot be empty.

4. Tap **Domain** and enter the domain on the touch-screen. Tap **OK**.

   The solution can be configured to NOT prompt for the domain (Login with Windows without specifying the domain).
5. Tap **Login**.

Register card with PUK code

1. Use the card reader.

   If the card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.
2. Enter the PUK code on the keypad or touch-screen.
3. Tap **PIN code** and enter the PIN code on the keypad or touch-screen.
4. Tap **PIN code** again and enter the PIN code again on the keypad or touch-screen.

The card is now registered with the user.

Ricoh Aficio MP 171, SP 201F, SP 201SPF

The control panel is as follows:
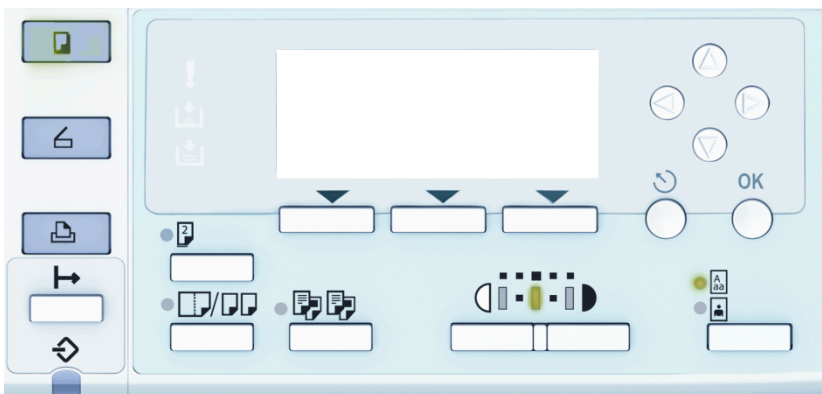
Login with card

Use the card reader.

Pull Print

Press the print button to print all non-retained documents.

ⓘ Retained documents cannot be printed on such devices.

Copy

Press the **Copy** button and then the **Start** button to copy the documents placed in the automatic document feeder (ADF).

Logout

Press the **Logout** selection key.

Using SafeCom P:Go Ricoh

Pull Print

- Use the card reader.

> ⓘ As there is no communication with the device's display, the user's name or credits are not displayed.

If there are documents to be printed, the data LED starts flashing and the documents are printed.

The user is logged out.

Troubleshooting

SafeCom Go Ricoh Device Trace Facility

Use the SafeCom Go Ricoh Information web page (Information web page) to collect information from the device, such as version and last printer states.

The SafeCom Go Ricoh log facility is also useful in troubleshooting situations, but it should only be enabled upon request from SafeCom support personnel. The log facility is enabled on the SafeCom Go Ricoh Log web page (Log web page).

SafeCom Help Desk Assistant

We want your SafeCom solution to be one that reduces not only print costs, but is also easy to support. In the following you will find useful troubleshoot hints. The most common problems reported by end-users have been compiled into an online SafeCom Help Desk Assistant available at safecom.eu/help.

SafeCom Administrator: Cannot add Pull Device with no MAC Address

If the SafeCom Administrator reports "Cannot add pull device with no MAC address", then do the following:

1. Open a web browser and enter the printer's address.

   JavaScript (Active Scripting) must be enabled.
2. Click **Login**, enter the Login User Name (admin) and the Login Password (by default, there is no password), then click **Login**.
3. Click **Configuration** on the left menu.
4. Under Network, click **IPv6**.
5. For IPv6, click **Disable**.
6. For Stateless Address Auto Configuration, click **Disable**.
7. Click **OK**.
8. Restart the printer.

If the above still fails, then install the software through the web page (Install SafeCom Go Ricoh through web page).

Unable to save changes to driver list

If running Internet Explorer 9, Compatibility View must be enabled to be able to save changes to the drivers list in the Ricoh web interface.

In Internet Explorer, open the **Tools** menu and select **Compatibility View**.

Unable to detect USB reader

If your Ricoh device is unable to detect a USB card reader, do the following:

1. Have your Ricoh technician bring the device into SP mode.

2. SP-5075-001 USB keyboard: set to 0

3. Commit changes by pressing the # key

For Ricoh devices using JVM v12, you may need the Vendor ID and Product ID of the card reader. Connect your card reader to a PC, and check the IDs under **Device Manager** > **Human Interface Devices** > **USB Input Device** > **Properties** > **Details** > **Property: Hardware IDs**.

After you determined the card reader IDs, set the device accordingly, entering the IDs:
* On the device itself, under **User tools** > **Login as Administrator** > **System Settings** > **General features – Next > Program** > **Change USB Device list**, or
* On the device configuration webpage, under **Device Management** > **Configuration** > **Program** > **Change USB Device list**.

When you are finished setting the IDs, reconnect the card reader to your Ricoh device.

The Vendor ID for all Elatec readers is 09D8.

The Product IDs for various Elatec readers are as follows:
* TWN3 Keyboard: PID 0310
* TWN3 Virtual COM Port: PID 0320
* TWN3 SafeCom (Report): PID 0206
* TWN4 Keyboard: PID 0410
* TWN4 CDC: PID 0420
* TWN4 SafeCom (Report): PID 0406

The Kofax MX Reader uses TWN4 PID.

USB reader unresponsive

If the USB card reader attached to your Ricoh device is not working, switch to using the back USB slot on the device, as the USB slot on the front panel of newer Ricoh devices may not recognize the device correctly.

Device looping on login screen

If you configure SafeCom Go to use card readers for authentication, and there is no card reader attached to the device, the attached card reader is not supported, or a physical keyboard is attached to the device, the device may loop between the login screen and displaying an "Unknown user" error message. To fix the issue, attach a card reader supported by SafeCom (see SafeCom ID devices).

Device stuck due to paper jam

If there is a paper jam in the ADF, the Ricoh device may become stuck on the "Copying" screen. In such cases, you have to manually delete the stuck job from the Job List.

Device displaying "Out of order" error when changing encryption length

On certain Ricoh devices, setting either the Asymmetric or Symmetric encryption keys to their maximum length (2048 and 256, respectively) may result in the connection timing out before the device decrypts the key. In such cases, lower the key length.

SafeCom Go webpage unreachable on the device

If you cannot access the SafeCom Go webpage of your Ricoh device, ensure the following:

- The Device Certificate is not expired (**Device Management** > **Configuration** > **Security – Device Certificate**). If the certificate is expired, create a new, valid device certificate.
- The SSL/TSL – IPv4 and IPv6 setting is inactive (**Device Management** > **Configuration** > **Security – SSL/TSL**). If the setting is active, disable it.

Alternatively, you can use the exact address of the various SafeCom pages:

- Information page: `http://{device IP}:8080/safecom?url=information`
- Configuration page: `http://{device IP}:8080/safecom?url=configuration`
- Register page: `http://{device IP}:8080/safecom?url=register`
- Log page: `http://{device IP}:8080/safecom?url=log`

- **Language page:** `http://{device IP}:8080/safecom?url=language`
- **Password page:** `http://{device IP}:8080/safecom?url=changepasswd`
- **Advanced page:** `http://{device IP}:8080/safecom?url=advanced`

SafeCom Go webpage not accessible on sleeping device

On some devices, the SafeCom Go webpage may become inaccessible if the device enters sleep mode. In such cases, the administrator can remotely wake up the device by browsing to the Web Image Monitor configuration UI of the device and selecting **Configuration** > **Extended Features Info**. This wakes up the device and makes the SafeCom Go webpage accessible.

Chapter 6

Regulatory information

WARNING NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures

* Reorient or relocate the receiving antenna.
* Increase the separation between the equipment and receiver.
* Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
* Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Changes or modifications not expressly approved by Kofax, Inc. could void the user's authority to operate this equipment according to part 15 of the FCC rules.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to take whatever measures may be required to correct the interference at the user's own expense.

CE conformance: This product has been developed and produced in accordance with the EMC directive and the Low Voltage directive and therefore carries the CE mark.

EMC directive: This product observes the rules and regulations of the EMC directive. If so required, a declaration of conformity in local language stipulating the applied rules and regulations can be obtained.