

Kofax SafeCom Go Fuji Xerox

Administrator's Guide

Version: 9.12.0

Date: 2020-12-11

The logo for KOFAX, consisting of the word "KOFAX" in a bold, blue, sans-serif font.

© 1995-2020 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of contents

Preface	4
Related documentation	4
Training.....	4
Getting help for Kofax products.....	4
Introduction	6
SafeCom Go Fuji Xerox	6
Requirements.....	6
Supported ID devices	6
Install SafeCom Go Fuji Xerox.....	8
Fuji Xerox ApeosPort-V, -IV, -III	8
Create certificate on the printer	8
Enable HTTPS on the printer.....	8
Add the device in SafeCom Administrator	8
Display Pull Print and Register icons.....	8
Install card reader on the printer.....	9
Connect the card reader	10
Configure the printer to use card reader	10
SafeCom Go Fuji Xerox - Device Server	11
Install SafeCom Device Server:.....	11
Windows Firewall - Ports that must be opened.....	11
Configure SafeCom Device Server	13
Log in to SafeCom Device Server	13
Add SafeCom Server	13
Device Server config.ini	14
Add device to the SafeCom Device Server	15
Add device in SafeCom Administrator.....	15
Add device via the SafeCom Device Server	17
Device icons.....	18
Configure device in SafeCom Device Server.....	19
Check device properties.....	22
Uninstall SafeCom Go Fuji Xerox.....	23
Enable SafeCom Mobile Pull Print	23
Control user access rights.....	23
Using SafeCom Go Fuji Xerox	24
Control panel	24
Login.....	24
Pull Print - Document list	24
Copy.....	25
E-mail.....	25
Register card with PUK code	25
Logout.....	26
Troubleshooting	27
Introduction	27
SafeCom Help Desk Assistant.....	27
Servlets.....	27
SafeCom Device Server does not start	27
Device server with multiple network cards.....	27
Device Server: Configuration of devices failed.....	28
Device Server: Error when upgrading existing Device Server installation.....	28
At the device: avoid having to press Enter when logging in without PIN.....	28
Device error message: "Login failed. Incorrect authentication server settings..."	28

Device error message: "Unable to configure device because: Device is in use,
retrying..." 29
Device error message: "Unable to configure device because: Missing licenses" 29

Regulatory information..... 30

Preface

This guide includes instructions for installing and using Kofax SafeCom Go Fuji Xerox.

Related documentation

The full documentation set for Kofax SafeCom Go Fuji Xerox is available at the following location

<https://docshield.kofax.com/Portal/Products/SafeCom/10.530-jaah72kksf/SafeCom.htm>

In addition to this guide, the documentation set includes the following items:

SafeCom Smart Printing

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

SafeCom G4

- *Kofax SafeCom G4 Administrator's Guide*
A comprehensive guide 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 Fuji Xerox

- *Kofax SafeCom Go Fuji Xerox User's Guide*
User's guide on how to use SafeCom Go Fuji Xerox.

Training

Kofax offers both classroom and online training to help you make the most of your Kofax solution. To learn more about training courses and schedules, visit the [Kofax Education Portal](#) on the Kofax website.

Getting help for Kofax products

The [Kofax Knowledge Base](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the [Kofax website](#) and select Support on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.
- Type your search terms or phrase into the Search box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
- Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.
- Access to the Kofax Customer Portal (for eligible customers).
- Click the Customer Support link at the top of the page, and then click Log in to the Customer Portal.

- Access to the Kofax Partner Portal (for eligible partners).
- Click the Partner Support link at the top of the page, and then click Log in to the Partner Portal.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

Scroll to the General Support section, click Support Details, and then select the appropriate tab.

Introduction

SafeCom Go Fuji Xerox

SafeCom Go Fuji Xerox is a solution for Fuji Xerox MFPs. It integrates with the touch-screen control panel of the Fuji Xerox MFP and offers user authentication by code and/or card.

SafeCom Go Fuji Xerox 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, scalable solutions.

Requirements

- SafeCom Go Fuji Xerox supports ApeosPort MFPs listed here: https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices.
- The Fuji Xerox MFP must be equipped with the External Access Kit from Fuji Xerox.
- SafeCom device license.
- SafeCom G4 server or SafeCom G3 server.
- SafeCom Device Server version S82 060.020*02 or later.
- The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.6 or later. It can be downloaded from www.java.com.

Note On ApeosPort-V devices, ensure that the Chain Link value of 701-436 is set to 0 for proper authentication behaviour. If you are unsure on how to perform this, contact your Fuji Xerox representative.

Supported ID devices

The SafeCom Serial to RS422 converter (p/n 688110) is required to connect the Fuji Xerox MFP with any of the serial SafeCom ID devices listed below:

Table 1 Supported SafeCom ID Devices

Identification Method	Card Reader Serial p/n
Windows authentication / ID code	
SafeCom AWID Reader	696010
SafeCom Barcode Reader*	694010
SafeCom Casi-Rusco Reader	652010
SafeCom EM Reader [E]	674110
SafeCom Felica Reader	697410
SafeCom HID Reader 35 bit [E]	673110
SafeCom HID Reader 37 bit	671110
SafeCom iCLASS Reader [E]	654110
SafeCom Indala Reader 26 bit	670010
SafeCom Indala Reader 29 bit	651010
SafeCom IoProx	658010
SafeCom Legic Reader [E]	679110
SafeCom Magnetic Card Reader (Tr 1)* **	959010
SafeCom Magnetic Card Reader (Tr 2)* **	954010
SafeCom Magnetic Card Reader (Tr 3)* **	657010
SafeCom Mifare Reader [E]	970110
SafeCom Nedap Reader	978990
SafeCom NexWatch Reader	698010

* Currently not working with Fuji Xerox.

** There are a maximum of 32 characters for Magnetic Card Readers.

Note 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.

Install SafeCom Go Fuji Xerox

Fuji Xerox ApeosPort-V, -IV, -III

The Device Administrator user name and password is required to log in:

User name	11111
Password	x-admin

Create certificate on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. To check if a valid certificate is already established click **Certificate Management** on the menu and then **Display the list**. If a certificate is established, proceed to Enable HTTPS on the printer.
3. Click Create New Self Signed Certificate.
4. Complete the details required for the Self Signed Certificate. Increase **Days of Validity** to the maximum allowed.
5. Click **Apply**.

For the certificate to work properly, you need to disable verification of remote server certificate:

1. On the printer's web page, click the **Properties** tab.
2. In the left menu click **Security** and then **SSL/TLS Settings**.
3. For Verify Remote Server Certificate uncheck the Enabled check box.
4. Click **Apply**.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **SSL/TLS Settings**.
3. Check **HTTP – SSL / TLS Communication** and verify that Port Number is 443.
3. Click **Apply**.
4. Click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Add the device in SafeCom Administrator

1. Make sure the SafeCom G4 Server software installation has been completed as described in the *SafeCom Smart Printing Administrator's Quick Guide*.
2. Make sure that the SafeCom Device Server is installed and running (3).
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Device Server. Remember to select **SafeCom Go Fuji Xerox** as the type of device. Alternatively the device can be added in **SafeCom Device Server** (see Add device via the SafeCom Device Server).

Display Pull Print and Register icons

Display the Pull Print icon on the printer's main screen:

1. On the printer press the **Log in/out** button.
2. Tap the user icon and change user to **System Administrator**.

3. Enter user name (default: 11111) and tap **Next**.
4. If prompted for a password, enter this as well (default: x-admin) and tap **Enter**.
5. Tap **Tools**.
6. Under **Group**, tap **Common Service Settings**.
7. Under **Features**, tap **Screen / Button Settings**.
8. Tap **7. Services Home**¹ and tap the **Change Settings** button.
9. Tap the position where you want the **Pull Print** icon to appear on the printer's main screen. Choosing a position that is currently listed as **(Not Assigned)** is recommended.

Note The numbering of the positions starts from the upper left corner and continues to the right.

10. Select **Web Application Server 1** and then tap **Details...** to verify that it is indeed **Pull Print**. Otherwise open and verify the details of **Web Application Server 2**.
11. Tap **Close** to close the details of the **Pull Print** web application.
12. Tap **Save**.
13. Tap **Save**.
14. Tap **Close**.
15. Tap **Close**.

Display the Register icon on the printer's main screen:

1. Follow the steps 1-8 of "Display the Pull Print icon on the printer's main screen".
2. Tap the position where you want the **Register** icon to appear on the printer's main screen. Choosing a position that is currently listed as **(Not Assigned)** is recommended.
3. Select **Web Application Server 1** and then tap **Details...** to verify that it is indeed **Register**. Otherwise open and verify the details of **Web Application Server 2**.
4. Tap **Close** to close the details of the **Register** web application.
5. Tap **Save**.
6. Tap **Save**.
7. Tap **Close**.
8. Tap **Close**.

Remove the icons from the printer's main menu:

1. Follow the steps 1-8 of "Display the Pull Print icon on the printer's main screen" above.
2. Select **Web Application Server 1** or **Web Application Server 2** and tap the **Details** button to verify that it is the web application you want to remove from the printer's main screen.
3. Scroll to the top of the list and select **(Not assigned)**.
4. Tap **Save**.
5. Tap **Save**.
6. Tap **Close**.
7. Tap **Close**.

Install card reader on the printer

Note ID devices require unique ID Device Licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for 3rd party ID devices must be purchased separately.

This section is only relevant if users will log in by card.

After a card reader is installed it is still possible to log in by entering an ID code if the user starts the login sequence by pressing the **Log In/Out** button.

Note The length of an ID code is maximum 32 characters instead of 39.

¹ **Services Home** is called **All Services** on ApeosPort-III devices.

Connect the card reader

1. Power off the printer.
2. Connect the serial SafeCom ID device to the SafeCom Serial to RS422 converter.
3. Connect the SafeCom Serial to RS422 converter to the provided SafeCom cable.
4. Connect the provided SafeCom cable to the RS422 port on the rear of the printer.
5. Power on the printer.

Configure the printer to use card reader

1. Log in as **Service Rep.** on the printer (if you do not know how, contact your Fuji Xerox representative).
2. Tap **Tools**.
3. In **Group** tap **Common Service Settings**.
4. In **Features** scroll to and tap **Maintenance/Diagnostics**.
5. Tap **NVM Read/Write**.
6. Change the three values according to the table below:

NVM/ Chain Link	Value (no reader)	Value (reader)
850-001	0	1
850-007	0	10
850-015	0	1

Note On ApeosPort-V devices, ensure that the Chain Link value of 701-436 is set to 0 for proper authentication behaviour. If you are unsure on how to perform this, contact your Fuji Xerox representative.

7. Tap **Save** after each value has changed.
8. Tap **Close**.
9. Tap **Exit (Keep Log)**.
10. Tap **Yes**.
11. Tap **Reboot Now**.
12. Power off the printer.

SafeCom Go Fuji Xerox - Device Server

Pre-requisites:

Make sure the SafeCom G4 Server software installation has been completed as described in the *SafeCom Smart Printing Administrator's Quick Guide*.

Install SafeCom Device Server:

1. Download the safecom_device_server_nnn.exe file from the link supplied to you. The installation must be **Run as administrator**. When the installation program is launched click **Next**.

Note If your device fleet includes HP Pro devices, ensure that the HP Pro devices are using a dedicated device server, and select the **Install only HP Pro** option for that device server on the **SafeCom Go Selection** screen. Otherwise, select the **Install without HP Pro** option.

2. Choose the destination folder for the files. Click **Next**.

The default installation folder is:

```
C:\Program Files\  
SafeCom\SafeCom Device Server
```

On **Windows 64-bit**:

```
C:\Program Files (x86)\  
SafeCom\SafeCom Device Server
```

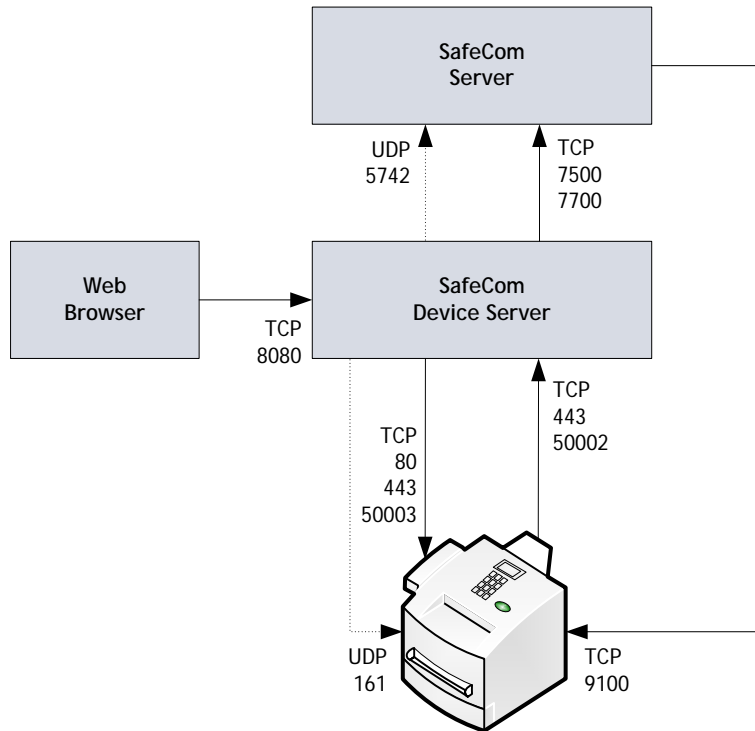
3. Click **Next**.
4. Choose destination folder. Click **Next**.
5. Detecting Java version. Click **Next**.
6. Review settings before copying of files starts. Click **Next**.
7. Click **Finish**.

Windows Firewall - Ports that must be opened

If Windows Firewall is enabled it may prevent the SafeCom solution from working. Disable the firewall or run the script below.

1. Browse to the SafeCom Device Server installation folder.
2. Right-click open_firewall_safecom_device_server.cmd. The command file must be **Run as administrator**. In the file you can see what TCP and UDP ports will be opened.

You can also manually ensure that the port numbers below are open.



TCP	Inbound on SafeCom Device Server	Protocol
80	Used to contact MFP during initial setup	HTTP
443	Used to contact MFP during operation	HTTPS
8080	Web browser	HTTP
50002	Device	HTTPS
UDP	Inbound on SafeCom Device Server	Protocol
161	Used to register notifications	SNMP
TCP	Outbound on SafeCom Device Server	Protocol
443	Used to contact MFP during operation	HTTPS
7500	SafeCom Server (Job Server)	SafeCom
7700	SafeCom Server (Job Server)	SafeCom
50003	Device	HTTPS
UDP	Outbound on SafeCom Device Server	Protocol
5742	SafeCom Server (Broadcast Server)	SafeCom
TCP		Protocol
9100	Used for printing	RAW

Configure SafeCom Device Server

The SafeCom Device Server must be configured manually to reference the right SafeCom Server. This is done by adding the SafeCom Server in the SafeCom Device Server. Furthermore a list of failover SafeCom Servers can be set up.

Log in to SafeCom Device Server

To log in to SafeCom Device Server:

1. Open a web browser and enter the server address (IP address or hostname) for the device server followed by :8080/safecom in the address field.

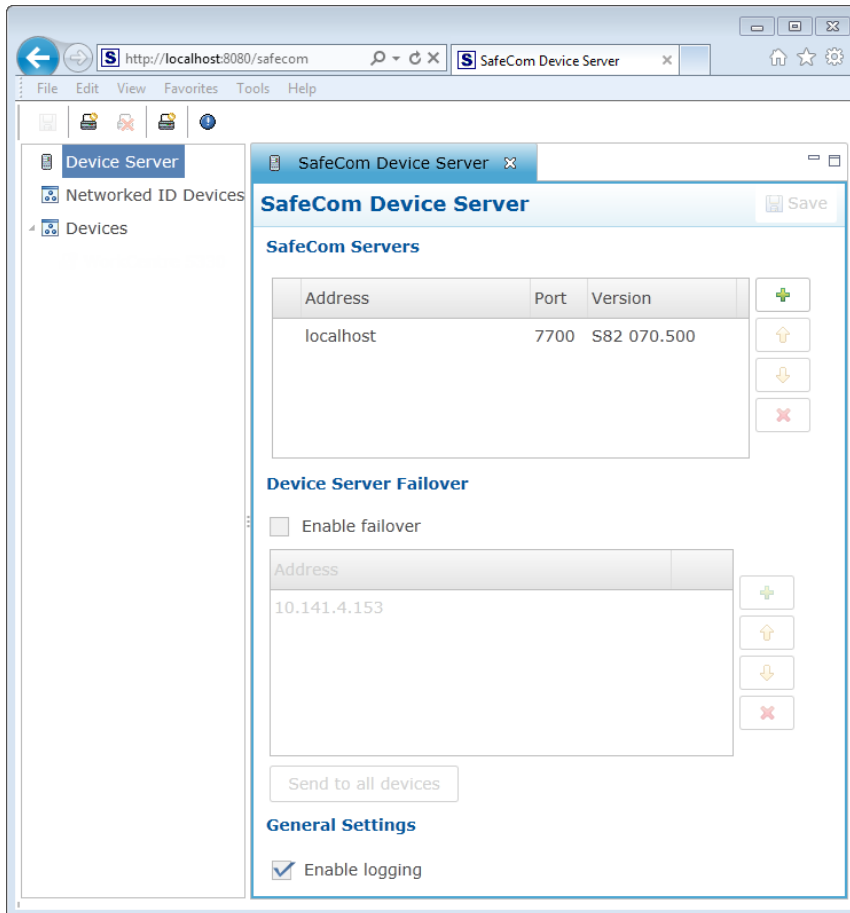
Example: `http://localhost:8080/safecom`

Note Use of JavaScript (Active Scripting) must be enabled.

2. Enter **Username** (default is admin) and **Password** (default is nimda).
3. Click **OK**. If a **Limited access** dialog opens, click **OK**.

Add SafeCom Server

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click **Device Server** in the menu to the left.



3. Under **SafeCom Servers**, click the **[+]** icon to add a failover SafeCom Server.
4. Enter the server address and click **OK**. To add localhost as the server, leave the **Address** field blank and click **OK**.

5. Click **Save**.

Note To use device server failover, group your devices via SafeCom Administrator. Device servers belonging to the same group monitor the status of the group members, and in case of a group member failing or shutting down, the rest of device server group distributes the workload of the downed device server among the rest. For more information, see section 5.14.4. Grouping device servers in the *SafeCom G4 Administrator's Manual*.

The SafeCom Server is now added, and the next step is to add a device to the device server.

Device Server config.ini

The following settings can be set by modifying the config.ini file located in the <installdir>/equinox folder.

After editing the config.ini file, the SafeCom Device Server service must be restarted for the changes to take effect.

Note Do not use Windows Notepad, as it will mangle line endings. WordPad, or another editor that understands Unix line endings are recommended. Editing the config.ini must be done with due diligence as it otherwise will break the runtime.

Setting	Description	Default
<code>deviceserver.encryptconfig</code>	Defines if configuration file is encrypted: 'true'=enable, 'false'=disable.	true
<code>deviceserver.configureddevices</code>	Option to disable the configuration code against devices. Useful mostly for testing purposes to support simulated devices.	true
<code>deviceserver.trace</code>	If set to 'true' it enables the server trace files	false
<code>deviceserver.protocol.trace</code>	If set to 'true' it enables the safecom protocol trace files	false
<code>deviceserver.serverAddress</code>	Sets the address that the devices must refer to.	InetAddress.getLocalHost()
<code>deviceserver.config.dir</code>	Sets the location of the configuration directory	config
<code>deviceserver.trace.file.size</code>	Defines the max size of each trace file. Defined in bytes but takes a postfix for larger units: KB, MB or GB	10MB
<code>deviceserver.trace.file.count</code>	Defines the number of old trace files to keep.	5
<code>deviceserver.thirdparty.trace.file.size</code>	Defines the max size of each third party trace file. Defined in bytes but takes a postfix for larger units: KB, MB or GB. Set only if needed.	N/A
<code>deviceserver.thirdparty.trace.file.count</code>	Defines the number of third party trace files to keep. Set only if needed.	N/A

Add device to the SafeCom Device Server

There are two ways of adding a device to the SafeCom Device Server:

- Via the SafeCom Administrator.
This is the recommended method and it works for SafeCom G3 Server version S82 070.410*05 or newer.
- Via the SafeCom Device Server web page.
Solutions based on SafeCom G2 must use this method.

Add device in SafeCom Administrator

Before adding a device server device in SafeCom Administrator a **SafeCom Device Server** must be added to the SafeCom.


If the device server is not yet added in the SafeCom Administrator, see the instructions above ([Configure SafeCom Device Server](#)) for configuring a SafeCom Device Server and adding it to a SafeCom Server. If the device server is already added in the SafeCom Administrator, go to **Add device server device** below.

Note To delete the device server you right-click the device server and select **Delete device server**, then click **OK**.

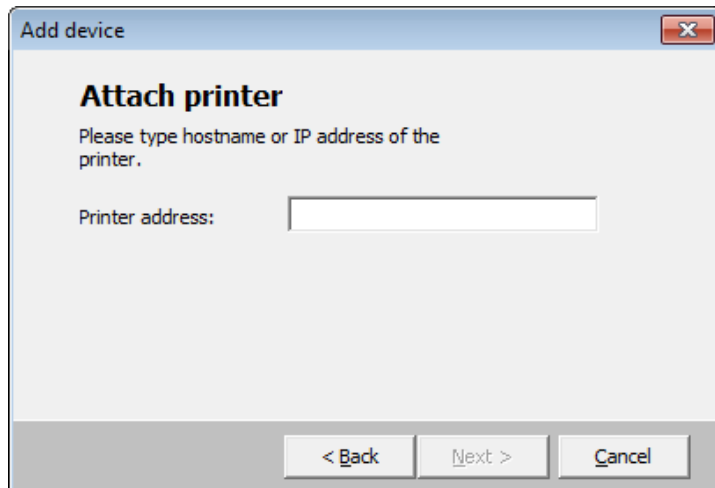
The SafeCom Device Server is now added to SafeCom Administrator and you can now add a device.

Add device server device

1. Click the **Devices** container, right-click the content area and then **Add device**. The **Add device wizard** is now launched.
2. From the **Device server** menu, select the **SafeCom Device Server** and click **Next**.



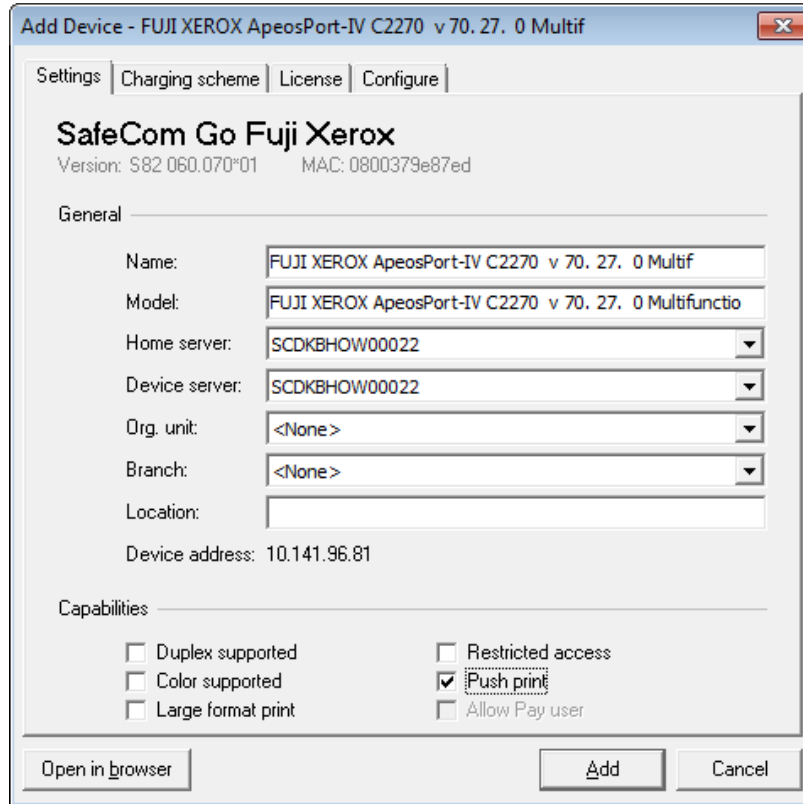
3. Information is retrieved from the device server to establish the status of device server. Click **Next**.
4. Enter the **Printer address** (the device IP address or host name) and click **Next**.



5. Information is then retrieved from the device. Click **Next**.
6. Now select **SafeCom Go Fuji Xerox** as the type of device and click **Next**.

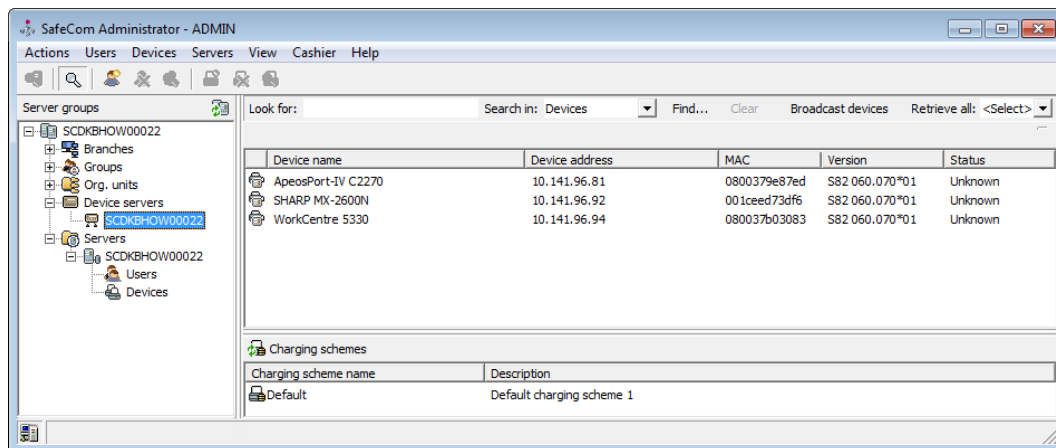


7. Enter the username and password, as specified on the device web page and click **Next**.
8. The device properties dialog now opens. Make sure to specify on the **Settings** tab the device server and the capabilities of the device.




9. Click **Add** to register the device and save it in the database. After approx. 2 minutes the device is added to the device server and available to be configured in **SafeCom Device Server**.

The device server device is now added and listed both under **Devices** and under the specific device server under **Device servers**.



10. Now proceed to configure SafeCom Go Fuji Xerox in the SafeCom Device Server.

Add device via the SafeCom Device Server

1. Click **Device Server** in the left menu.
2. Click the **Add device**  button and the **Add device wizard** launches.
3. Enter the hostname or the IP address of the device. If you want to use dynamic IP address, then enter the device hostname in the **Address** field.
4. Click **Next**.


The screenshot shows a window titled "Add Device" with a subtitle "Enter basic device information". It contains four text input fields: "Address:", "Administrator name:", "Administrator password:", and "SNMP Get Community:". The "SNMP Get Community" field has the value "public" entered. At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

5. Information is retrieved from the device to establish the type of device. Make the necessary adjustments to the **Required Device properties**.

The screenshot shows the "Add Device" window at the "Retrieved Device Information" step. It displays the following information: Hostname: 10.141.96.81, MAC Address: 0800379E87ED, Description: ApeosPort-IV C2270, Location: (empty), Model: FUJI XEROX ApeosPort-IV C2270 v 70. 27. 0 Multifunction System. Below this is a section titled "Required Device properties" containing a table with the following data:

Key	Value
LockCopy	skip
LockFax	skip
LockPrint	skip
LockScan	skip
LoginWithoutPIN	false
UseSSL	true







At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

6. Click **Finish**.
7. On the device settings page, make sure the settings are correct.
8. Click **Save** .

Note The device is now added to the SafeCom solution, but it does not appear in the **SafeCom Administrator** until a user logs in at the device.

Device icons

Once the devices are added in the SafeCom Device Server the following device icons represents the status of the devices.


-  User is logged in at the device.
-  Device is idle, no user logged in.
-  Wait for at least 2 minutes. If the warning signal is gone, the printer is now configured. If the warning signal remains, the printer cannot be configured because, for example the SSL is not on, or another device server is trying to configure the printer.
-  An error occurred.
-  The printer is receiving print data.
-  Device server cannot contact the printer.

Configure device in SafeCom Device Server

The **Device** tab is used to configure SafeCom Go Fuji Xerox as to which device it is connected to, how users are to be identified etc.

Note If the configuration of the devices fails it might be because the Device Server is installed on a server that has multiple NICs or IPs. Refer to [Device Server: Configuration of devices failed](#) for a resolution.

To save any changes you make to the configuration, click **Save** in the upper right corner of the web page.

Expect between 60 and 90 seconds for the saved changes to take effect if they involve changes to selected setting like the **Login method**. During the update, the device icon has a yellow warning sign  and the device shows the text: **Now Remote Operating. Please do not turn off the Power.**

Device: ApeosPort-IV C2270
Save

Device Settings

Model: FUJI XEROX ApeosPort-IV C2270 v 70. 27. 0 Multifunction System
 MAC Address: 0800379EB7ED
 Device Message: Unable to configure device because: Device is configured against a different server (10.141.112.5)

Device information

Manufacturer: Contact:
 Location: Description:

Network settings

Address: SNMP get community:
 RAW print port: SNMP put community:

Device settings

Administrator name: Administrator password:
 Login method: Default domain:
 Language:

Hide domain
 Enable post tracking
 Reverse document list
 Mask ID code

▸ Drivers

▸ Device properties

Property Key	Property Value
LockCopy	skip
LockFax	skip
LockPrint	skip
LockScan	skip

Enable logging

Change the settings according to the following descriptions:

- **Device information**
 - **Manufacturer** and **Description** are automatically filled-in and together with **Location** they are also viewable in the **Device properties** dialog in **SafeCom Administrator**.
 - **Contact** and **Location** provides useful information in maintaining the SafeCom solution.
 - **Network settings**
 - **Address:** The IP address of the device.
 - **RAW print port:** The TCP port used to send print data.
 - **SNMP Put Community name:** This must match the SNMPGet Community Name if this is different from public. By default SNMP GetCommunity name is public.
 - **Device settings**
 - **Administrator name:** The user name with which the administrator can log in to device.
 - **Administrator password (mandatory):** The device password with which the administrator can log in to device.
 - **Login method:** This determines how users log in. Choose between:
 - **Card**
 - **ID code**
 - **Card or ID code**
 - **Card or Windows:** Allows the user to log in by either card or by entering their Windows username, password, and domain.

Note Identification by card requires connecting a USB ID Device (card reader). The option **Card or Windows** allows the user to log in by either card or by entering their Windows username, 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).
- Note** The **Default domain** setting will only take effect after the domains list has been refreshed on the device, or the device has been restarted. To refresh the domains list, follow these steps:
1. On the device press the **Login** button.
 2. Press the **Domains/Realms** button.
 3. Press **Refresh domains**.
 4. Press **Save**.
 5. Press **Cancel**. The next time the domains list is shown on the device the default domain is set.
- **Language:** Specify a specific language if you want SafeCom Device Server to override the language on the device.
- **Hide domain:** Check to allow the users to log in without specifying the domain.
- **Enable post tracking:** This is relevant only with SafeCom Tracking. Refer to the *SafeCom G4 Administrator's Manual*.
- **Reverse document list:** Check to show the first printed documents at the top of the document list.
- **Mask ID code:** Check to mask the ID code with asterisk (*) when entered at the device.
- **Drivers:** When Pull Printing, SafeCom compares the driver name embedded in the print job with its list of driver names. If no match is found and if **Show fidelity warning** is checked in the **Server properties** in the **SafeCom Administrator**, the document appears with a question mark [?] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.

- Click **Get All** to obtain the list of drivers from the SafeCom Server, or add and delete drivers manually.
 - **Device Properties:**
 - **LockCopy:** If set to **True** only logged in users are allowed to use the function. Enter **False** to allow all users to access the function. Enter **Skip** to go with the settings already set on the device.
 - **LockFax:** If set to **True** only logged in users are allowed to use the function. Enter **False** to allow all users to access the function. Enter **Skip** to go with the settings already set on the device.
 - **LockPrint:** If set to **True** only logged in users are allowed to use the function. Enter **False** to allow all users to access the function. Enter **Skip** to go with the settings already set on the device.
 - **Lock Scan:** If set to **True** only logged in users are allowed to use the function. Enter **False** to allow all users to access the function. Enter **Skip** to go with the settings already set on the device.
 - **UseSSL:** Set to **True** to use SSL.
 - **LoginWithoutPIN:** set to **True** to allow logging in without a PIN.
 - **Enable logging:** Select if log information should be collected.
- Note** The device will always log performance data (network latency, authentication duration of successful logins, number of **Out of order** occurrences and duration, failover and fallback between G4 servers, device reboots, changes in firmware and Go versions).
- **Restore factory default:** Set all settings to their default value. Except from the password.
 - **Reconfigure device:** Reference the device to the current SafeCom Device Server.

Check device properties

If the device was added via the **SafeCom Device Server** it was also added to the SafeCom solution and appears in the list of devices in **SafeCom Administrator**.

To update the device properties in the **SafeCom Administrator**:

1. Click Start, point to All Programs, SafeCom G4, and click SafeCom Administrator.
2. In **SafeCom Administrator** click on the server to login.
3. Enter **User logon** (default is ADMIN) and **Password** (default is nimda).
4. Open the list of devices. If the device you added is not present press F5 to refresh the list. Double-click the device to open the **Device properties** dialog.
5. On the **Settings** tab make the appropriate changes. Make sure that the Home server and Device server are specified and that **Duplex supported** and **Color supported** is set correctly.
6. On the **Charging scheme** tab select the appropriate charging scheme.
7. On the **License** tab check the appropriate licenses.
8. Click **OK**.

The screenshot shows the 'Add Device' dialog box for a FUJI XEROX ApeosPort-IV C2270. The 'Settings' tab is selected, displaying the following configuration:

- Name:** FUJI XEROX ApeosPort-IV C2270 ;ESS1.102.4,IOT 70.
- Model:** FUJI XEROX ApeosPort-IV C2270 ;ESS1.102.4,IOT 70.2
- Home server:** SCDKBHOW00022
- Device server:** SCDKBHOW00022
- Org. unit:** <None>
- Branch:** <None>
- Location:** (empty field)
- Device address:** 10.141.96.81

Capabilities:

- Duplex supported
- Color supported
- Large format print
- Restricted access
- Push print
- Allow Pay user

Buttons at the bottom: 'Open in browser', 'Add', and 'Cancel'.

Uninstall SafeCom Go Fuji Xerox

To uninstall the SafeCom Go Fuji Xerox software from the device:

1. Open a web browser and login to the **SafeCom Device Server**.
2. Click **Device server** in the menu and select the device from which the SafeCom Go solution must be uninstalled.
3. Click the **Delete** icon in the top menu to uninstall.
4. Click **Save**.

Enable SafeCom Mobile Pull Print

To allow users to Pull Print documents via their smart phone, a QR code must be printed for each device. Users then scan the QR code label at the device with their phone, thus identifying themselves and declaring their presence at the specific device.

For details on how to print a QR code for the device, refer to the *Kofax SafeCom G4 Administrator's Guide*.

Make sure that the default domain is configured on the device in SafeCom Device Server (see [Configure device in SafeCom Device Server](#)), 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).

For more details on how to Pull Print from a smart phone refer to the *SafeCom Mobile Pull Print User's Guide*.

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 via SafeCom Administrator, refer to the *Kofax SafeCom G4 Administrator's Guide*. You can control access rights to the following features:

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

Note If either scanning or e-mailing is enabled a user will have access to both functions.

Using SafeCom Go Fuji Xerox

Control panel



Login

Note If a card reader is installed it is still possible to login by entering an ID code if the user starts the login sequence by pressing the Log In/Out button.

Login with card:

1. Use card reader.

Login with card and PIN code:

1. Use card reader.
2. Enter **PIN code** and tap **Enter**.

Login with ID code:

1. Enter **ID code** on the screen and tap **Next**.
2. Tap **Enter**

Note The length of an ID code is maximum 32 characters.

Login with ID code and PIN code:

1. Enter **ID code** on the screen and tap **Next**.
2. Enter **PIN code** and tap **Enter**.

Login with Windows:

1. Enter **Username** and tap **Next**.

Note If domains are used, you can either tap the **Domain** button to select domain or you can enter the domain as part of the user name as either "user@domain" or "domain\user".

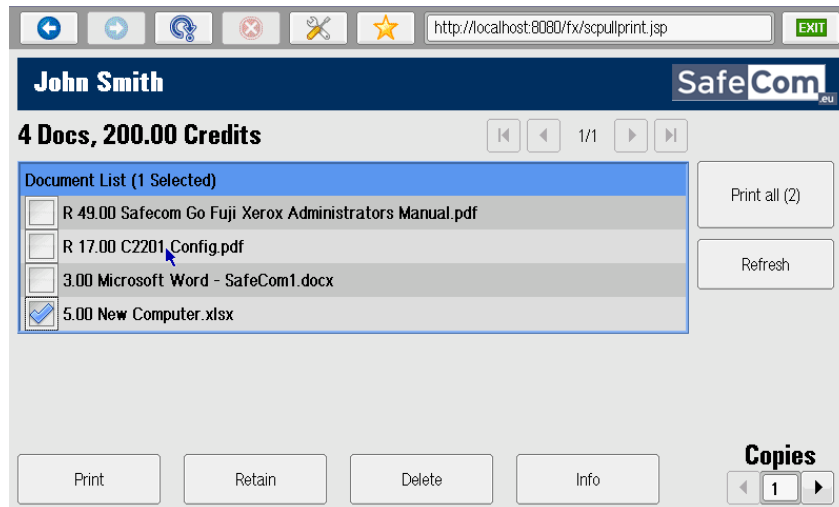
2. Enter **Password** and tap **Enter**.

Pull Print - Document list

Access the **Document list** that allows you to print individual documents.

1. Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. If **Print all at login** is checked any documents pending collection will be printed first.



In the above example the 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**.

- 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** to see 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 has finished spooling after the user logged in.
- Press **Services Home**² to go back to the previous screen.
- Tap **Copies** to request multiple copies of a document. **Print all** will always be one copy of each document.

Copy

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

E-mail

Tap the **E-Mail** button. Tap **Add Me** and then press the **Start** button to scan and e-mail the document to the e-mail address of the logged in user.

Register card with PUK code

² **Services Home** is called **All Services** on ApeosPort-III devices.

1. Enter the ID code with which you want to register the card. The ID code must be unknown to SafeCom and a PUK code must be available in the system.
2. The user is logged in but all functions are locked.
3. Tap the **Register** button.
4. Enter the PUK code and the PIN code.
5. Tap **OK** and the card is registered with the entered ID code.

Note When registering card with PUK code, the user might be asked to enter a PIN code as well even if login without PIN is enabled for the user. This depends on the settings on the device as they bypass the settings on the **User properties** in **SafeCom Administrator**.

Logout

To log out:

- Use card reader if the user logged in with card.
- Press the **Log In/Out** button.

Troubleshooting

Introduction

This chapter contains troubleshooting hints for the SafeCom Go Fuji Xerox product. Additional troubleshooting hints are available in the Troubleshooting chapter in the *Kofax SafeCom G4 Administrator's Guide*.

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 section, you will find useful troubleshooting hints.

Servlets

SafeCom has implemented two servlets to improve diagnostics data in **SafeCom Device Server**:

- /debug/dump/heap
- /debug/dump/threads

Enter the path to the **SafeCom Device Server** in a browser followed by the paths to the servlets.

Example: `http://<DeviceServerAddress>:8080/debug/dump/heap`

Note These servlets have been implemented in order to assist SafeCom Support in diagnosing severe failures regarding SafeCom Device Server. Therefore, we recommend only making the thread and heap dump on request from SafeCom Support Technician.

SafeCom Device Server does not start

The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.6 or later. You can download it from www.java.com.

Device server with multiple network cards

If you have multiple network cards attached to the computer running the SafeCom Device Server, by default the SafeCom Device Server tells devices to contact it at the IP address of the first available network card.

To manually set the IP or hostname to use, do the following:

1. Open the folder `equinox` inside the SafeCom Device Server installation folder.
2. Edit the file `config.ini`.
3. At the bottom of the file, add the following line, replacing `x.x.x.x` with the correct IP address or hostname:
`Deviceserver.serverAddress=x.x.x.x`
4. Open **Services** and restart the SafeCom Device Server.

Device Server: Configuration of devices failed

If the Device Server is installed on a server that has multiple NICs or IPs, the configuration of devices may fail.

This is because the Device Server uses the IP returned by Java, which may be problematic if the IP returned to the Device Server is unavailable (because of network layout) from the devices point of view.

A solution is to configure the property `deviceserver.serverAddress` in the `config.ini` file. This forces the Device Server to use the given IP when configuring devices. Refer to [Device Server config.ini](#).

Device Server: Error when upgrading existing Device Server installation

The following error might appear when upgrading an existing Device Server installation:

"Error in action StopWindowsService"

The following must be completed before running the installer again:

1. Kill the installer process with the following command:

```
taskkill /F /IM scDeviceServer.exe
```

2. Stop the SafeCom Device Server Service with the following command:

```
net stop scDeviceServer
```

3. Start the SafeCom Device Server again with the following command:

```
net start scDeviceServer
```

4. Re-run the SafeCom Device Server installer.

At the device: avoid having to press Enter when logging in without PIN

If you want to ensure that users logging in with a card do not need to press Enter when the device displays a dialog requesting a PIN code, ensure that the **Login without PIN code** checkbox is marked on the **User Properties** page of SafeCom Administrator for all users allowed to login without PIN code.

Device error message: "Login failed. Incorrect authentication server settings..."

If the message "Login failed. Incorrect authentication server settings..." appears when a user tries to login after rebooting, it is possible that the device is still configuring, why the user should try again later.

Device error message: “Unable to configure device because: Device is in use, retrying...”

On some old device models (AP-III, AP-IV for example), adding the device to the Device Server via SSL may fail, resulting in the above error message. In such cases, set the **UseSSL** property to “**false**” for the device on the Device Server web page.

Device error message: “Unable to configure device because: Missing licenses”

This message refers to a device license/feature missing on the device. The missing piece could be one of the following features:

AUTH_AGENT
REMOTE_AUTHENTICATION
CUSTOM_SERVICE
WEB_UI

Please consult with a Fuji-Xerox engineer to confirm that all these features are available on the device.

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 SafeCom a/s 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 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.