

Kofax SafeCom Go Fuji Xerox Administrator's Guide

Version: 9.13.0

Date: 2023-05-03

KOFAX

© 1995-2023 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	5
Training.....	5
Getting help with Kofax products.....	5
Chapter 1: Introduction	7
SafeCom Go Fuji Xerox.....	7
Requirements.....	7
SafeCom ID devices.....	7
Chapter 2: Install SafeCom Go Fuji Xerox	9
Fuji Xerox ApeosPort-V, -IV, -III.....	9
Create certificate on the printer.....	9
Enable HTTPS on the printer.....	9
Add the device in SafeCom Administrator.....	10
Display Pull Print and Register icons.....	10
Install card reader on the printer.....	11
Connect the card reader.....	11
Configure the printer to use card reader.....	12
Chapter 3: SafeCom Go Fuji Xerox - Device Server	13
Install SafeCom Device Server.....	13
Windows firewall – Ports that must be opened.....	13
Configure SafeCom Device Server.....	15
Log in to SafeCom Device Server.....	15
Add SafeCom Server.....	16
Device Server config.ini.....	17
Add device to the SafeCom Device Server.....	18
Device icons.....	19
Add device through the SafeCom Administrator.....	19
Add device through the SafeCom Device Server.....	20
Configure device in SafeCom Device Server.....	20
Check device properties.....	24
Uninstall SafeCom Go Fuji Xerox.....	24
Enable SafeCom Mobile Pull Print.....	25
Control user access rights.....	25
Chapter 4: Using SafeCom Go Fuji Xerox	26
Control panel.....	26

Login.....	26
Log in with card.....	26
Log in with card and PIN code.....	26
Log in with ID code.....	26
Log in with ID code and PIN code.....	27
Log in with Windows.....	27
Pull Print - Document list.....	27
Copy.....	28
E-mail.....	29
Register card with PUK code.....	29
Logout.....	29
Chapter 5: Troubleshooting.....	30
SafeCom Help Desk Assistant.....	30
Servlets.....	30
SafeCom Device Server does not start.....	30
Device server with multiple network cards.....	31
Device Server: Configuration of devices failed.....	31
Device Server: Error when upgrading existing Device Server installation.....	31
At the device: avoid having to press Enter when logging in without PIN.....	32
Device error message: "Login failed. Incorrect authentication server settings".....	32
Device error message: "Unable to configure device because: Device is in use, retrying".....	32
Device error message: "Unable to configure device because: Missing licenses".....	32
Chapter 6: Regulatory information.....	33

Preface

This guide is intended for administrators who are responsible for integrating Kofax SafeCom software for use with Fuji Xerox MFP devices.

Training


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

Getting help with 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:

1. Go to the [Kofax website](#) home page and select **Support**.
2. When the Support page appears, select **Customer Support > Knowledge Base**.

 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.

From the Knowledge Base home page, you can:

- Access the Kofax Community (for all customers).
Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).

Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.

- Access the Kofax Partner Portal (for eligible partners).

Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.

- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

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

Chapter 1

Introduction

SafeCom Go Fuji Xerox

SafeCom Go Fuji Xerox is a solution for Fuji Xerox MFPs. It integrates with the touchscreen control panel of the Fuji Xerox MFP and offers user authentication by code 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 higher.
- The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.6 or higher. It can be downloaded from www.java.com.


i 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.

SafeCom 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:

Supported SafeCom ID devices

Identification Method	Card Reader Serial p/n
Windows authentication / ID code	
SafeCom AWID Reader	696010
SafeCom Barcode Reader ¹	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) ^{1 2}	959010
SafeCom Magnetic Card Reader (Tr 2) ^{1 2}	954010
SafeCom Magnetic Card Reader (Tr 3) ^{1 2}	657010
SafeCom Mifare Reader [E]	970110
SafeCom Nedap Reader	978990
SafeCom NexWatch Reader	698010

 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 Currently not working with Fuji Xerox.

² There are a maximum of 32 characters for Magnetic Card Readers.

Chapter 2

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:

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.
4. Click **Apply**.
5. Click **OK** to restart the device's web server.

6. Click **Reboot Machine**.
7. 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. For more information, see [SafeCom Go Fuji Xerox - Device Server](#).
3. In **SafeCom Administrator**, use **Add device** to add the SafeCom Device Server.
4. Select **SafeCom Go Fuji Xerox** as the type of device.
Alternatively, the device can be added in **SafeCom Device Server** (see [Add device through the SafeCom Device Server](#)).

Display Pull Print and Register icons

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

1. Press the **Log in/out** button on the printer.
2. Tap the user icon and change user to **System Administrator**.
3. Enter user name (the default is 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**³ 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. Selecting a position that is currently listed as **(Not Assigned)** is recommended.

 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 set to **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 from 1 to 8 in [Display the Pull Print icon on the printer's main screen](#) section.


³ **Services Home** is called **All Services** on ApeosPort-III devices.

2. Tap the position where you want the **Register** icon to appear on the printer's main screen. Selecting 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 set to **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 from 1 to 8 in [Display the Pull Print icon on the printer's main screen](#) section.
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

 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, log in by entering an ID code is still possible if the user starts the login sequence by pressing the Log In/Out button.

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


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. Tap **Save** after each value has changed.

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

 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 **Close**.
8. Tap **Exit (Keep Log)**.
9. Tap **Yes**.
10. Tap **Reboot Now**.
11. Power off the printer.

Chapter 3

SafeCom Go Fuji Xerox - Device Server

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

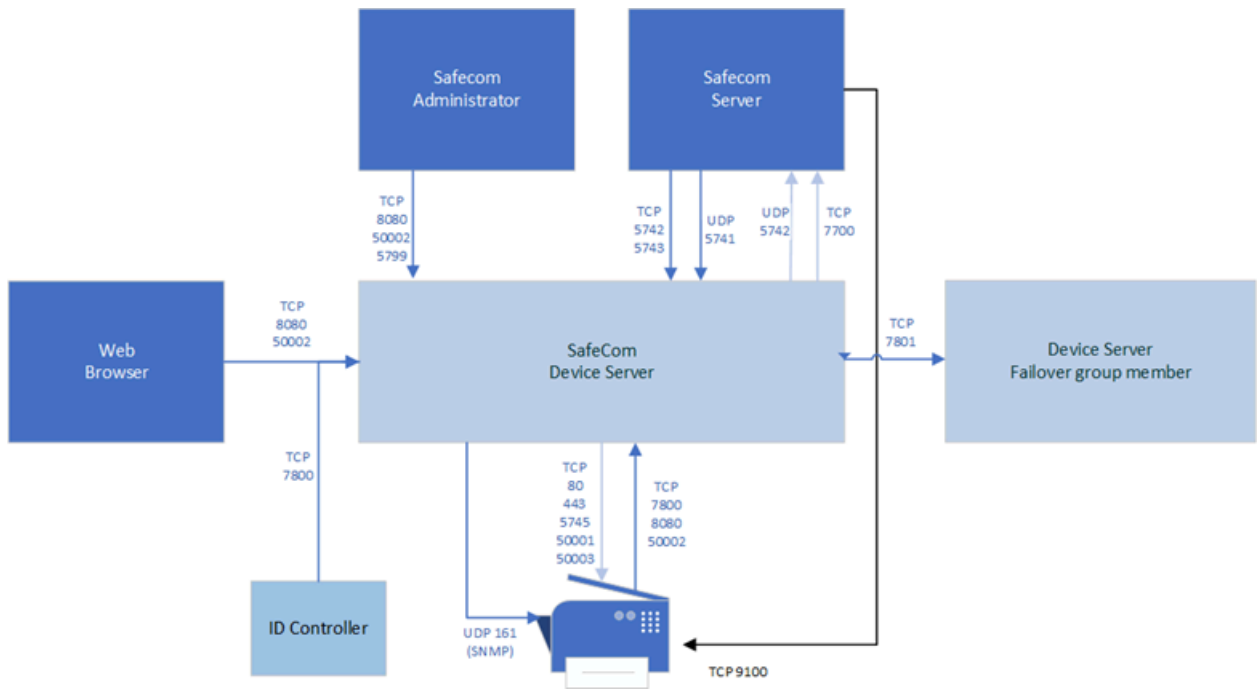
1. Download the `SafeCom_Device_Server_x64_build_{version_number}.exe` file from the link supplied to you. The installation must be **Run as administrator**.
2. When the installation program is launched, click **Next**.
3. Select the destination folder for the files. Click **Next**.
The default installation folder is `C:\Program Files\SafeCom\SafeCom Device Server`.
4. Click **Next**.
5. Review settings before copying of files starts. Click .
6. Click **Finish**.

Windows firewall – Ports that must be opened

If Windows Firewall is enabled, it may prevent the SafeCom Device Server from working. Disable the firewall or run the following script:

1. Browse to the **SafeCom Device Server** installation folder.
2. Right-click `open_firewall_safecom_device_server.cmd` and select **Run as administrator**.
You can see the opened TCP and UDP ports in the file.

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




Inbound connections

5741	UDP	SafeCom Server: SafeCom identification
5742	TCP (RAW)	SafeCom Server: Push requests
5743	TCP (TLS 1.2)	SafeCom Server: Push requests (version 9.13 and later)
5799	TCP (RAW)	SafeCom Administrator (versions earlier than 10.6): Device status
7800	SafeCom (TCP)	SafeCom ID controller
7801	TCP (RAW)	Failover: data exchange
8080	HTTP	Device Server Web Configurator SafeCom Administrator (versions earlier than 10.6): device configuration MFP
8081	HTTP	HP OPS Server for HP Pro devices (legacy)
50002	HTTPS	SafeCom Web Configurator SafeCom Administrator (version 10.6 or later): device configuration and device status MFP

Outbound connections

161	SNMP (UDP)	Device discovery
443	HTTPS	Used to contact MFP during operation
5742	UDP	SafeCom identification (SafeCom G4 Server / Broadcast Server)
5745	TCP	HP Jedi call back
7627	HTTP	HP Jedi Web services (unsecure)
7700	TCP	SafeCom Server (Job Server), Configurable to 7500 Protocol: <ul style="list-style-type: none"> • Version 9.13 and later - Configurable TLS 1.2 or SafeCom • Versions earlier than 9.13 - SafeCom
7801	TCP (RAW)	Failover: data exchange
50001	HTTPS	MFP
50003	HTTPS	MFP (Konica Minolta)

 Make sure that the firewall script provided with G4 server is also executed and all necessary ports are open.

Configure SafeCom Device Server

SafeCom Device Server needs an active SafeCom G4 Server to work properly. If Device Server is installed on a computer running SafeCom G4 Server, then the components connect to each other automatically. Otherwise the connection must be established manually using the Device Server configuration page.

Log in to SafeCom Device Server

1. Open a web browser and enter the following URL to access the Device Server configuration page:

`https://[hostname or IP address]:50002/safecom`

Example: `https://localhost:50002/safecom`



- The use of JavaScript (Active Scripting) must be enabled.
- It is possible to use an unsecure HTTP port 8080 for this purpose (`http://localhost:8080/safecom`).

2. Enter the SafeCom Administrator's 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 on the left.



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

The screenshot above indicates that the local SafeCom G4 Server is automatically connected.

If several servers are added to the list, then their order can be managed by the arrow buttons and any of them can be deleted by the [x] button. The server on the top of the list serves as the primary connection for the Device Server. The other servers get in use if the primary server is out of order. The first available one is connected in this case. Once the primary server becomes available again, Device Server connects to it automatically.

5. Configure the communication protocol. This can be custom SafeCom protocol (Legacy) or TLS 1.2.

Legacy protocol must be selected if the connected version of SafeCom servers is earlier than 10.520.10, or the TLS communication is disabled on at least one server. Otherwise TLS connection is recommended.

If both protocols are enabled, TLS is the preferred encryption. Legacy protocol is used if the G4 server does not support TLS.



- The protocol switch controls the channel encryptions between Device Server and PrintClient in the same manner.
- If the peers support TLS, but the connection cannot be established (for example, due to a TLS handshake problem, or when TLS 1.2 is not enabled), then the Legacy connection will not be used. The issue with the TLS connection must be resolved, or the TLS protocol must be disabled on the configuration page of Device Server.
- The encryption settings are common for all added G4 servers and for print clients as well.

6. Optionally, you can enable the Device Server logging feature for diagnostic purposes.

7. When all settings are configured, click **Save**.

This page can be visited at any time to change the connection settings. The asterisk after the protocol type indicates the actual protocol in use. If the protocol settings are changed, the SafeCom Device Server service must be restarted.



Device Server instances can be organized into failover groups in SafeCom Administrator. Device Servers belonging to the same group monitor the status of the group members, and when a group member fails or shuts down, the device server group distributes the workload of the downed device server among the rest of the group members. For more information, see the *Group device servers* section in the *SafeCom Administrator* chapter of [SafeCom G4 Server Administrator's Guide](#). Check the ports used by SafeCom Device Server (see [Windows firewall – Ports that must be opened](#)) to ensure the communication between group members.

The SafeCom Server is now added, and devices can be added to the device server.

Device Server config.ini

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

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



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

Setting	Description	Default
deviceserver.encryptconfig	Defines if configuration file is encrypted. 'true'=enable 'false'=disable	true
deviceserver.configureddevices	Option to disable the configuration code against devices. Useful mostly for testing purposes to support simulated devices.	true
deviceserver.trace	If it is set to 'true', it enables the server trace files.	false
deviceserver.protocol.trace	If it is set to 'true', it enables the SafeCom protocol trace files.	false
deviceserver.serverAddress	Sets the address that the devices must refer to.	InetAddress.getLocalHost()
deviceserver.config.dir	Sets the location of the configuration directory.	config
deviceserver.trace.file.size	Defines the maximum size of each trace file. Defined in bytes but takes a postfix for larger units: KB, MB, or GB.	10MB
deviceserver.trace.file.count	Defines the number of old trace files to keep.	5
deviceserver.thirdparty.trace.file.size	Defines the maximum 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
deviceserver.thirdparty.trace.file.count	Defines the number of third party trace files to keep. Set only if needed.	N/A
deviceserver.includedProtocols	TLS/SSL protocols can be enabled for 3rd party Jetty component with this setting. For old models of KM devices, SSLv2Hello protocol must be enabled using this value: SSLv3,TLSv1,TLSv1.1,TLSv1.2,SSLv2Hello (Comma separated list with no whitespaces).	Empty string. Jetty enables each SSL/ TLS protocol except SSLv2Hello.







Add device to the SafeCom Device Server

The device can be added to the SafeCom Device Server in one of the following two ways:

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

Device icons


In the SafeCom Device Server, the following device icons represent the status of the device.

Icon	Description
	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.

Add device through the SafeCom Administrator

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

If the device server is not yet added in the SafeCom Administrator, see the instructions above 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 the steplist below.

 To delete the device server, 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 add a device.

Add a device server device

1. Click the **Devices** container, right-click the content area and select **Add device**.
The Add Device Wizard appears.
2. From the **Device server** menu, select the **SafeCom Device Server** and click **Next**.
Information is retrieved from the device server to establish the status of the device server.
3. Click **Next**.
4. Enter the **Printer address** (the device IP address or host name) and click **Next**.
Information is retrieved from the device.
5. Click **Next**.
6. Select **SafeCom Go Fuji Xerox 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, then click **Next**.
The device properties dialog box opens.



8. 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 approximately 2 minutes, the device is added to the device server and is available to be configured in the **SafeCom Device Server**.

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

10. Go to the [Configure device in SafeCom Device Server](#) section to continue with the configuration of the device.


Add device through the SafeCom Device Server

1. Click **Device Server** in the left menu.
2. Click the **Add device**  button.
The Add Device Wizard appears.
3. Enter the hostname or the IP address of the device.
If you want to use dynamic IP address, enter the device hostname in the **Address** field.
4. Enter the administrator name and password for the device and click **Next**.
Information is retrieved from the device to establish the type of device.
5. Make the necessary adjustments to the **Required Device properties**.
6. Click **Finish**.
7. On the device settings page, make sure the settings are correct, then click **Save** .

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

Configure device in SafeCom Device Server

The **Device** tab is used to configure SafeCom Go Fuji Xerox with regards to which device it is connected to, how users are to be identified, and so on.

 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. See [Device Server: Configuration of devices failed](#) for a resolution.

Device Settings

Manufacturer: Fuji Xerox
 Model: FUJI XEROX ApeosPort-VI C3371 v 50. 65. 0 Multifunction System
 MAC Address: 1C7D221188DA
 Serial number: TC101167507124
 Device Message:

Device information

Contact: Location:
 Description:

Network settings

Address: RAW print port:
 Select SNMP version:
 SNMP get 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
LoginWithoutPIN	false
UseSSL	true

Enable logging


Restore factory default

Reconfigure device


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".

Change the settings according to the following descriptions:

Option	Description
Device information	<ul style="list-style-type: none"> • 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 provide useful information in maintaining the SafeCom solution.
Network settings	<ul style="list-style-type: none"> • Address: The IP address of the device. • RAW print port: The TCP port used to send print data. • Select SNMP version: These properties must match the SNMP settings of the device. First, select the SNMP version configured on the device. The SNMP related fields change according to the selected version. <ul style="list-style-type: none"> • SNMP v2: Provide SNMP Get and Put Community name. The default value of these properties is public. • SNMP v3: Provide the Username, select the Authentication protocol and enter the passphrase, select Privacy Protocol and enter the passphrase
Device settings	<ul style="list-style-type: none"> • 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. Select one of the following: <ul style="list-style-type: none"> • 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. <div data-bbox="634 1409 1450 1591" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> 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.</p> </div> • 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 in domain\username format.

Option	Description
	<p>i 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:</p> <ol style="list-style-type: none"> 1. Press the Login button on the device. 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. <ul style="list-style-type: none"> • Language: Specify a specific language if you want SafeCom Device Server to override the language on the device. • Hide domain: Usable if you specified a default domain. Check it to allow the users to log in without typing in the domain. • Enable post tracking: This is relevant only with SafeCom Tracking. For more information, see the <i>SafeCom G4 Administrator's Manual</i>. • Reverse document list: Check it to show the first printed documents at the top of the document list. • Mask ID code: Check it to mask the ID code with asterisk (*) when entered at the device.
Drivers	<p>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 of 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.</p>
Device Properties	<ul style="list-style-type: none"> • LockCopy: If it is 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 it is 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 it is 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 it is 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 it to True to use SSL. • LoginWithoutPIN: Set it to True to allow logging in without a PIN.

Option	Description
Enable logging	Select if log information should be collected.  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).
Restore factory default	Set all settings to their default value, except for the password.
Reconfigure device	Reference the device to the current SafeCom Device Server.

Check device properties

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

Perform the following steps 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**.

Uninstall SafeCom Go Fuji Xerox

Perform the following steps 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 on the top menu to uninstall.
4. Click **Save**.

Enable SafeCom Mobile Pull Print

1. To allow users to Pull Print documents through their smart phone, a QR code must be printed for each device.

Users can 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, see the *Kofax SafeCom G4 Administrator's Guide*.

2. 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 in domain\username format.

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

Control user access rights

When using SafeCom G3 server version S82 070.440*03 or higher, you can control users' access rights to specific features through SafeCom Administrator. For more information, see the *Kofax SafeCom G4 Administrator's Guide*. You can control access rights to the following features:

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

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

Chapter 4

Using SafeCom Go Fuji Xerox

Control panel



Login

i If a card reader is installed users can to login by entering an ID code if they start the login sequence by pressing the Log In/Out button.

Log in with card

Use card reader.


Log in with card and PIN code

1. Use card reader.
2. Enter **PIN code**.
3. Tap **Enter**.

Log in with ID code

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

3. Tap **Enter**.


 The length of an ID code is maximum 32 characters.

Log in with ID code and PIN code

1. Enter **ID code** on the screen.
2. Tap **Next**.
3. Enter **PIN code**.
4. Tap **Enter**.

Log in with Windows

1. Enter **Username**.

 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".

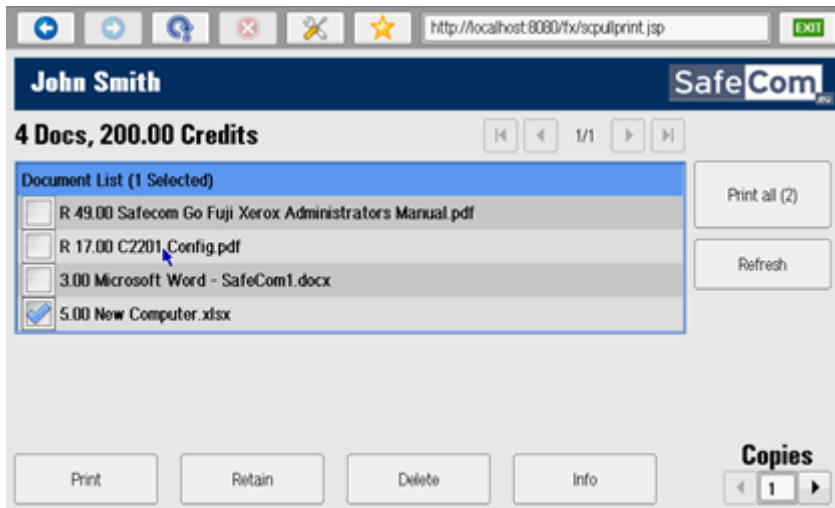
2. Tap **Next**.
3. Enter **Password**.
4. Tap **Enter**.

Pull Print - Document list

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

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.
- Tap Services Home⁴ to go back to the previous screen.
- Tap Copies to request multiple copies of a document. Print all always means printing 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).


⁴ Services Home is called All Services on ApeosPort-III devices.

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

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.

 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

Do one of the following to log out:

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

Chapter 5

Troubleshooting

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

Kofax 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.

For example: `http://{DeviceServerAddress}:8080/debug/dump/heap`

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

SafeCom Device Server does not start

The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.6 or higher. 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 `config.ini` file.
 - a. 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
```
3. 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 `deviceserver.serverAddress` property in the `config.ini` file. This forces the Device Server to use the given IP when configuring devices. For more information, see [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 check box is selected 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, so the user should try again later.

Device error message: "Unable to configure device because: Device is in use, retrying"

On some old device models, for example AP-III, AP-IV, adding the device to the Device Server through 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.

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.