

Kofax SafeCom Go Sharp 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 | 6 |
| Training..... | 6 |
| Getting help with Kofax products..... | 6 |
| Chapter 1: Introduction | 8 |
| SafeCom Go Sharp..... | 8 |
| Requirements..... | 8 |
| SafeCom ID devices..... | 9 |
| Sharp device passwords..... | 10 |
| Chapter 2: SafeCom Go Sharp - 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..... | 14 |
| Device Server config.ini..... | 15 |
| Add device to the SafeCom Device Server..... | 16 |
| Device icons..... | 17 |
| Add device through the SafeCom Administrator..... | 17 |
| Add device through the SafeCom Device Server..... | 18 |
| Configure device in SafeCom Device Server..... | 18 |
| Chapter 3: SafeCom Go Sharp - How to | 23 |
| Select login method..... | 23 |
| Enable copy..... | 23 |
| Enable e-mail..... | 24 |
| Control user access rights..... | 24 |
| Register device..... | 24 |
| Enable SafeCom Mobile Pull Print..... | 25 |
| Restore factory default..... | 25 |
| At the printer: SafeCom error message when coming out of power save..... | 26 |
| Uninstall SafeCom Go Sharp..... | 26 |
| SafeCom Go Sharp device trace facility..... | 27 |
| See the trace files generated by the Device Server..... | 27 |
| Configure the size and number of the trace files..... | 27 |
| Chapter 4: SafeCom Controller | 28 |

| | |
|--|-----------|
| Installation with SafeCom Controller..... | 28 |
| Write down the IP address of the device..... | 28 |
| Connect hardware..... | 28 |
| Add device in SafeCom Administrator..... | 29 |
| Configure the Sharp device web interface..... | 30 |
| Configure new Sharp devices..... | 30 |
| Sharp Web Interface (old models)..... | 32 |
| Configure the SafeCom Controller Web Interface..... | 33 |
| Log in to the SafeCom Controller Web Interface..... | 33 |
| Advanced Configuration web page..... | 33 |
| SafeCom web page..... | 33 |
| Printer web page..... | 34 |
| SafeCom Go for Controller - How to..... | 36 |
| Enable copy tracking for Controller..... | 36 |
| Specify SafeCom Server and device connection..... | 36 |
| Register device..... | 37 |
| Set password to prevent unauthorized access..... | 37 |
| Assign a fixed IP address to the SafeCom Controller..... | 37 |
| Select user identification..... | 37 |
| Disable the Test button..... | 38 |
| Enable Copy Control..... | 38 |
| Enable High Speed Print..... | 38 |
| Access Sharp MFP's System Settings..... | 38 |
| Restore factory default..... | 38 |
| Resend configuration..... | 39 |
| Uninstall SafeCom Go Sharp..... | 39 |
| Chapter 5: Using SafeCom Go Sharp..... | 40 |
| Sharp device with SafeCom Device Server..... | 40 |
| Login..... | 40 |
| Main menu..... | 41 |
| Pull Print - Document list..... | 41 |
| Copy..... | 42 |
| Account - Select billing code..... | 42 |
| Register card..... | 43 |
| Logout..... | 44 |
| Sharp MX devices with MX-AMX2 license..... | 44 |
| Login..... | 44 |
| Main menu..... | 45 |

| | |
|---|-----------|
| Pull Print - Document list..... | 45 |
| Copy..... | 46 |
| Account - Select billing code..... | 46 |
| Register card..... | 46 |
| Logout..... | 47 |
| Sharp device with SafeCom Controller..... | 48 |
| Control panel..... | 48 |
| Login..... | 48 |
| Main menu..... | 49 |
| Pull Print - Document list..... | 49 |
| Copy..... | 50 |
| Register card with PUK code..... | 50 |
| Logout..... | 51 |
| Chapter 6: Troubleshooting..... | 52 |
| SafeCom Help Desk Assistant..... | 52 |
| Servlets..... | 52 |
| SafeCom Administrator: Unable to locate all SafeCom devices..... | 52 |
| Copy jobs are not tracked..... | 53 |
| Print performance is slow..... | 53 |
| At the printer: No billing codes available..... | 53 |
| MFP reports: Could not access the accounting server..... | 53 |
| ERROR[5000]: Processing is in motion..... | 54 |
| Device Server: Configuration of devices failed..... | 54 |
| Device Server: Error when upgrading existing device server installation..... | 54 |
| Device Server: Pull Print icon is not available..... | 54 |
| SafeCom reader does not work..... | 55 |
| User auto logout does not work when the device goes to sleep on some Sharp devices..... | 55 |
| Chapter 7: Regulatory information..... | 56 |

Preface

This guide is intended for administrators who are responsible for integrating Kofax SafeCom software for use with Sharp 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 Sharp

SafeCom Go Sharp is the embedded solution for Sharp MFPs. It integrates with the touchscreen control panel of the Sharp MFP and offers user authentication by code or card.

SafeCom Go Sharp 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.

SafeCom Go Sharp is available in two variants:

- [SafeCom Device Server](#)

The software is installed on a server and an optional card reader, which supports keyboard, is connected to the USB port of the Sharp device.

- [SafeCom controller](#)

The SafeCom Controller hardware is connected to the network outlet and the Sharp device is connected to the spare network port of the SafeCom Controller. An optional card reader can be connected to either the USB or serial port of the SafeCom Controller.

Requirements

- SafeCom Go Sharp supports Sharp OSA (Open Systems Architecture) MFPs with Access Control. SafeCom Go is available in two variants, one that is software based (SafeCom Device Server) and one that is hardware based (SafeCom Controller). Supported devices are listed here: https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices
- The selected card reader (SafeCom ID device) must be supported by the SafeCom Controller / SafeCom Device Server.
- Sharp MFP must have a hard disk drive and a network card.
- Sharp MFP must have the latest available firmware version.
- Sharp product key for the Sharp External Account Module (MX-AMX3) must be registered on the MFP.
- Sharp AR models require Network Scanning Expansion Kit.
- SafeCom device license.

- The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.7 or later. It can run on the same physical hardware as the SafeCom Server. If SafeCom Device Server is installed on a 64-bit operation system, a Java version 32-bit needs to be installed. JRE can be downloaded from www.java.com.

SafeCom ID devices

SafeCom Go Sharp supported SafeCom ID devices

| Identification Method | USB SafeCom Controller | Serial SafeCom Controller | USB Keyboard SafeCom Device Server |
|--|------------------------|---------------------------|------------------------------------|
| Kofax MX Proximity Reader [USB, KBD] | | | SC0K970930 |
| SafeCom AWID Reader [R] | 696420 | 696010 | 696720 |
| SafeCom Barcode Reader | 694020 | 694010 | |
| SafeCom Casi-Rusco Reader [R] | 652420 | 652010 | 652720 |
| SafeCom Cotag Reader | 678020 | | |
| SafeCom EM Reader [E] | 674120 | 674110 | 674620 |
| SafeCom Felica Reader [R] | 697420 | 697310 | 697720 |
| SafeCom HID Prox Reader [R] | 673420 | 673310 | 673720 |
| SafeCom iCLASS Reader [R] | 654420 | 654310 | 654720 |
| SafeCom Indala Reader [R] | 670420 | 670010 | 670720 |
| SafeCom Indala Reader 29 bit [R] | 651020 | 651010 | 651720 |
| SafeCom Inditag [E] | 670120 | 670110 | 670620 |
| SafeCom IoProx Reader [R] | 658420 | 658010 | 658720 |
| SafeCom Legic Reader [R] | 679420 | 673310 | 679720 |
| SafeCom Magnetic Card Reader (Tr 1) | | 959010 | |
| SafeCom Magnetic Card Reader (Tr 2) | | 954010 | |
| SafeCom Magnetic Card Reader (Tr 3) | | 657010 | |
| SafeCom Magnetic Card Reader DD (Tr 1) | 692010 | | 692810 |
| SafeCom Magnetic Card Reader DD (Tr 2) | 691020 | | 691820 |
| SafeCom Magnetic Card Reader DD (Tr 3) | 692020 | | 692820 |
| SafeCom Mifare Reader [E] | 970120 | 970110 | 970620 |
| SafeCom Nedap Reader | 653020 | 978990 | |
| SafeCom NexWatch Reader [R] | 698420 | 698010 | 698720 |

i 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.

The ID device is either fitted or supplied with a 1.8 - 2.0 m cable. Additional information about the ID devices is available in the *SafeCom G4 Administrator's Guide*.

Sharp device passwords

Sharp device passwords

| Sharp MFP | New models | Old models: AR-M355, AR-M455, AR-M550, AR-M620, AR-M700, MX-M350, MX-M450, MX-M550, MX-M620, MX-M700 |
|-----------|------------|---|
| User name | admin | admin |
| Password | admin | Sharp |

Chapter 2

SafeCom Go Sharp - Device server

Make sure the SafeCom G4 Server software installation has been completed.

Install SafeCom Device Server

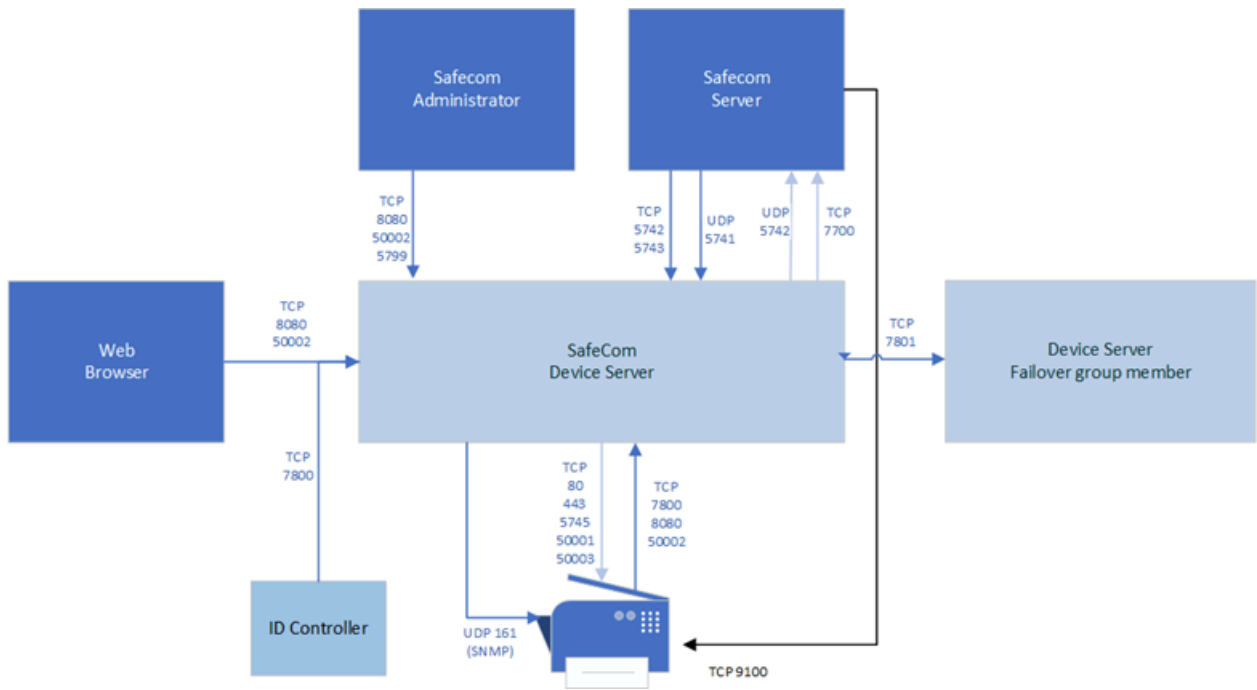
1. Download the SafeCom_Device_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be **Run as administrator**.
2. When the installation program is launched, click **Next**.
3. Select the destination folder for the files. Click **Next**.
The default installation folder is C:\Program Files\SafeCom\SafeCom Device Server.
4. Click **Next**.
5. Select destination folder. Click **Next**.
The installer detects the Java version.
6. Click **Next**.
7. Review settings before copying of files starts. Click **Next**.
8. 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) |

i 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 Sharp** 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** with the name SafeCom Device Server.

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**.
For more information, see *Configure device in SafeCom Device Server*.
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 Sharp 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: Sharp
 Model: SHARP MX-3100N
 MAC Address: 0022F3F7EFE1
 Serial number: 0801307100
 Device Message:

Device information

Contact: Location: Nuanco Budapest
 Description: PRN-SHP-3100N-539

Network settings

Address: 10.144.200.195 RAW print port: 9100
 Select SNMP version: SNMP2
 SNMP get community: public

Device settings

Administrator name: admin Administrator password: *****
 Login method: Card or ID Code Default domain:
 Language: (Auto) Idle timeout: 30 seconds

Hide domain
 Enable post tracking
 Reverse document list
 Mask ID code

Drivers

Device properties

| Property Key | Property Value |
|----------------------|----------------|
| AlternativeKeyboard | false |
| BillingEnabled | false |
| Dsk | false |
| NewModel | false |
| Reboot | true |
| SSL | false |
| serviceLogin | service |
| welcomeScreen | true |
| welcomeScreenTimeOut | 120 |

Device applications
 Enable user authentication and tracking per application

E-mail
 Copy
 Scan to USB

Enable logging


To save any changes you made 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".

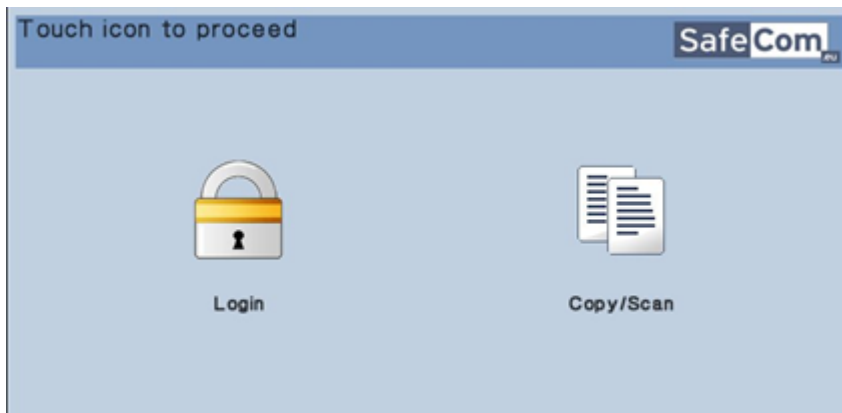
i If you click **Save** and then in the **Device Message** field see the message "Unable to configure device because: Device is configured against a different server", it is because the device is configured to a different server. To be able to make changes to the device configuration, you must first click **Reconfigure device** which configures the device to your server, make the necessary changes, and then click **Save**.

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 box in SafeCom Administrator. • Contact and Location provides 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 1528 1450 1709" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p>i 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 |

| Option | Description |
|--------------------------|---|
| | <p>the users are required to use domains, they can enter the domain with their username in domain\username format.</p> <ul style="list-style-type: none"> • Idle timeout: Specifies the time in seconds before automatically logging out a logged in user who does not show any activity. • Hide domain: Usable if you specified a default domain. Select this box 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 <i>SafeCom G4 Administrator's Manual</i>. • Reverse document list: Select this box to show the first printed documents at the top of the document list. • Mask ID code: Select this box 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 selected 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.</p> |
| Device Properties | <ul style="list-style-type: none"> • DSK: If the Device Security Kit is installed, DSK must be set to True, and the addresses for Application UI (<a href="http://<SafeCom Device server ip-address>:8080/safecomosa/go">http://<SafeCom Device server ip-address>:8080/safecomosa/go) and Web Service (<a href="http://<SafeCom Device server ip-address>:8080/services/safecomosa">http://<SafeCom Device server ip-address>:8080/services/safecomosa) must be entered manually on the device web page under Application Settings, External Application Settings, and then External Accounting Application Settings. • NewModel: Set the property value to True if you are adding a new Sharp model that has not yet been tested by SafeCom. The default value is False. • Reboot: This option is set to True, which means that the device automatically restarts. Set it to False if you want to restart the device manually. • SSL: Set this option to True to use SSL. • AlternativeKeyboard: Set this option to True to use the alternative keyboard. Use it if you encounter PIN/password masking issues due to the device display. • BillingEnabled: Set to True to display the Account icon on the device screen, allowing you to set up the billable account. Set to False to remove the icon. <div data-bbox="634 1566 1450 1688" style="background-color: #e0f2f7; padding: 10px; border: 1px solid #ccc;"> <p> If you set the BillingEnabled property on an already-configured device, you need to reconfigure the device for the change to take effect.</p> </div> <ul style="list-style-type: none"> • serviceLogin: This service password must correspond to the service password on the device. The default is "service". • welcomeScreen: Set the property value to True if you want the Welcome screen displayed at the device before user login. If the property value is False, then it is the login screen that is displayed for the user. The default value is True. |

| Option | Description |
|--------------------------------|---|
| | <p>i The property requires an AMX-3 license to work; devices with both AMX-2 and AMX-3 licenses do not display the screen set through this property.</p> <ul style="list-style-type: none"> • welcomeScreenTimeOut: Specify the time in seconds when the welcome screen should timeout. The default value is 120. • AlternativeKeyboard: Set the property value to True to use an alternative virtual keyboard for masking sensitive information (ID, PIN, and so on) on Sharp devices with older firmware. This may result in some rare language-specific characters being unavailable. |
| Device applications | <p>Specify if the users are allowed to Email, Copy, or Scan to USB without having to log in first. Select one or more of the three boxes to allow the users to perform these tasks without authentication.</p> <p>The settings in the Device applications are tied to the Welcome screen. If one or more of the Email, Copy, or Scan to USB boxes are selected, then the welcome screen only shows the option to Login and if enabled, Windows login. If none of the Email, Copy, or Scan to USB boxes are selected, the users have the option to Login and to Copy/Scan from the welcome screen.</p> |
| Enable logging | <p>Select if log information should be collected.</p> <p>i 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).</p> |
| Restore factory default | <p>Set all settings to their default value, except for the password. For more details, see Restore factory default.</p> |
| Reconfigure device | <p>Informs the device to reference the device to the current SafeCom Device Server.</p> |



Welcome screen

Chapter 3


SafeCom Go Sharp - How to

The following sections contain step-by-step instructions for some of the administrator's most common tasks.

Select login method

To set the method of user identification at the device:

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click on **Device server** in the menu on the left, and click on the device.
3. In **Login method** under **SafeCom Settings**, select how users must identify themselves at the device.
 - ID code
 - Card
 - Card or ID code (default)
 - Card or Windows

 When changing login method from Card or ID code to Card or Windows, the change will take effect after logging in and out on the device.

Enable copy

To enable SafeCom to do tracking on copy on the Device server:

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click on **Device server** in the menu on the left, and click on the device.
3. Click **Device applications**.
4. Select **Copy** in the list of applications.
5. Click **Save**.

Enable e-mail


To enable tracking on e-mails on the SafeCom Device server:

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click on **Device server** in the menu on the left, and click on the device.
3. Click **Device applications**.
4. Select **E-mail** in the list of applications.
5. Click **Save**.

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. For more information, see *SafeCom G4 Administrator's Guide*. You can control access rights to the following features:

- Copy
- Copy in color
- E-mail
- Scan
- Fax
- USB memory print
- USB memory scan
- Print all button

 Granting or denying access on a per feature level does not work due to device limitations. It is recommended to either set access to all features or to none of the features.

Register device

Register the device with the SafeCom solution in one of the following ways:

- Add the device in the SafeCom Administrator by using **Add device**.
- Log in at the device, if the user has Technician or Administrator rights.

Enable SafeCom Mobile Pull Print

Check the following:

- To allow users to Pull Print documents through 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, see the *SafeCom G4 Administrator's Guide*.

- Make sure that the default domain is configured on the 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 *SafeCom Mobile Pull Print User's Guide*.

Restore factory default

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click **Restore factory default** at the bottom of the web page.

The factory default values are:

Factory default values


| Configuration settings | Field | Default value |
|------------------------|--------------------|-------------------|
| Device settings | Model | |
| | MAC Address | |
| | Device Message | |
| User settings | Login Method | Card or ID code |
| | Idle timeout | 60 seconds |
| | Post tracking | Cleared (No) |
| Network settings | Address | Device IP address |
| | SNMP Get Community | Public |
| | SNMP Put Community | Private |
| | RAW print port | 9100 |
| Device information | Contact | |
| | Location | |
| | Description | |
| | Manufacturer | |
| Drivers | | |

| Configuration settings | Field | Default value |
|------------------------|----------------------|--------------------------------|
| Device properties | welcomeScreen | |
| | welcomeScreenTimeOut | 120 |
| | adminLogin | admin |
| | adminUserName | admin |
| | serviceLogin | service |
| | NewModel | false |
| | | Date and time of configuration |
| Device applications | E-mail | Selected (Yes) |
| | Pull Print | Selected (Yes) |
| | Copy | Selected (Yes) |
| | Scan to USB | Selected (Yes) |
| Logging | Enable logging | Selected (Yes) |

At the printer: SafeCom error message when coming out of power save

To avoid SafeCom error message when the device is coming out of power save mode, set Sleep Mode Power Level to Fast Wake up on the device web page.

1. Open the device in a web browser.
2. Under **Energy Saving Setting**, set **Sleep Mode Power Level** to **Fast Wake Up**.
3. Click **Save**.

 On Sharp MX-2610N, you need to be logged in as local administrator to access the setting.

Uninstall SafeCom Go Sharp

To uninstall the SafeCom Go Sharp software from the device server:

1. Open a web browser and log in 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 **OK** to confirm deleting the SafeCom solution.

SafeCom Go Sharp device trace facility

i Use the SafeCom trace facility only if Kofax Technical Support instructs you to do so.

Enable the trace facility through the SafeCom Device Server:

1. Open the SafeCom Device Server and log in.
2. Select a device in the device server pane and make sure that the **Logging enabled** box is selected at the bottom of the page.
3. Click **Save**.

See the trace files generated by the Device Server

1. Go to the destination folder for the log files:
The default installation folder is
 - On Windows 32-bit: `C:\Program Files\SafeCom\SafeCom Device Server\logs`
 - On Windows 64-bit: `C:\Program Files (x86)\SafeCom\SafeCom Device Server\logs`
2. If you need to send the log files, make sure to save and send the folder logs as a compressed/ zipped folder.

Configure the size and number of the trace files

1. Browse to the config.ini file:
 - On Windows 32-bit: `C:\Program Files\SafeCom\SafeCom Device Server\equinox\config.ini`
 - On Windows 64-bit: `C:\Program Files (x86)\SafeCom\SafeCom Device Server\equinox\config.ini`
2. Double-click the config.ini file. In the opened file, scroll to the bottom and add:
 - `deviceserver.trace.file.size` - to configure file size. Size is written as a number with an optional qualifier. For example, ten is 10 bytes, ten kilobytes is 10KB, ten megabytes is 10MB, and one gigabyte is 1GB.
 - `deviceserver.trace.file.count` - to configure how many trace files are generated. Enter the number of files you want to generate as a number.

After configuring the trace files, restart the SafeCom service.

Chapter 4

SafeCom Controller

Installation with SafeCom Controller

1. Make sure the SafeCom G4 Server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator**, use the **Add device** button to add the SafeCom Controller.
 - a. Select **SafeCom Go Sharp** as the type of device.
4. Configure the Sharp web interface.

Write down the IP address of the device

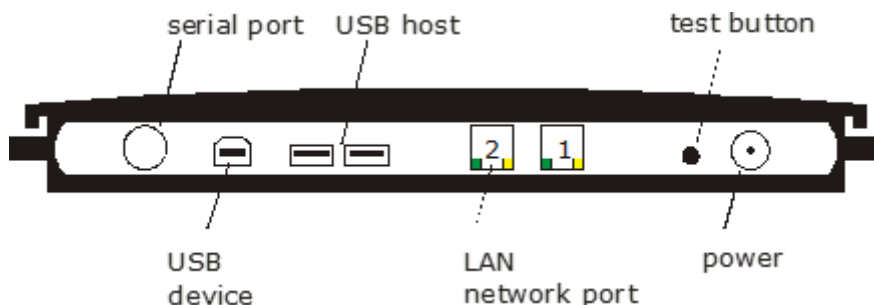
The IP address can normally be found in the device's control panel and on the configuration page. For more information, see the device's manual.

IP address /
hostname:

i The SafeCom Controller must reference the Sharp device by a fixed IP address or a fixed fully qualified hostname. For example: mysharp.safecom.eu.

Connect hardware

Make sure that the SafeCom software installation has been completed before you connect the hardware. When powered up, the hardware automatically discovers the server software.



SafeCom Controller's rear panel

1. Switch off the power to the device.
2. Connect a network cable to the **LAN** port on the rear panel of the SafeCom Controller. Connect the other end of the cable to the network.
3. Connect a network cable to the device. Connect the other end of the cable to the SafeCom Controller's other network port.
4. Connect the SafeCom Controller and the optional SafeCom Card Reader.
5. Connect the power supply to the SafeCom Controller.
When you power on, you must wait approximately 1 minute while SafeCom initializes.
6. Switch on the power to the device.

Add device in SafeCom Administrator

The SafeCom Controller's LAN light changes from flashing to on when an IP address is set. You need to determine the IP address of the SafeCom Controller so you can add it to the SafeCom solution.

Find IP address through broadcasting

Use SafeCom Administrator and its Broadcast function. However, broadcasting will not work if the SafeCom Controller is on a different VLAN.

Find IP address in the DHCP server

Login to the DHCP server and lookup the assigned IP address based on the MAC address. The MAC address of the SafeCom Controller is printed on the white label on the bottom of the SafeCom Controller. The MAC address is a 12-digit hexadecimal number, for example 00C076FF00F2.

1. Start **SafeCom Administrator**.
2. Login to the server by double-clicking its **Group name** listed to the left.
3. Enter **User logon** (default is ADMIN) and **Password** (default is nimda).
4. Add a device.
 - IP address known from DHCP server: Click **Add device** and proceed to step 7.
 - Find it through Broadcasting: Click on the **Find** button and select **Devices**.
5. Click **Broadcast....**
6. Right-click on the SafeCom Controller in the list and click **Add device**.

The Add Device Wizard appears.

7. Enter the **IP address** of the SafeCom Controller.

8. Click **Next**.


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

9. Click **[change]**.

10. Select **SafeCom Go Sharp** as the type of the SafeCom device.

11. Click **Next**.

12. Enter the **Printer address** (IP address or host name) of the Sharp device connected to the SafeCom Controller.

 The SafeCom Controller must reference the Sharp device by a fixed IP address or a fixed fully qualified hostname. For example, mysharp.safecom.eu.

13. Click **Next**.

Information is retrieved from the Sharp device.

14. Click **Next**.

15. For the device, enter the **User name** (default is admin) and **Password** (default is admin). On older devices, the default password is Sharp.

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

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

After approximately 1 minute, the SafeCom Controller is restarted and you can verify the connection to the Sharp MFP by pressing the **test** button once on the rear panel of the SafeCom Controller.

18. Configure the Sharp web interface.

Configure the Sharp device web interface

Configure new Sharp devices

Follow the steps below to configure the web interface on new Sharp devices. If you have an old Sharp device, see [Sharp Web Interface \(old models\)](#).

The web interface must be configured to allow communication with the SafeCom Go Sharp solution.


1. Open the Sharp device's web interface and login.

2. Enter the **User name** (default is admin) and **Password** (default is admin) for the device. On older devices the default password is Sharp.

3. Click **Login**.

4. Click **Application Settings**, and then **External Applications Settings**.

5. Click **External Accounting Application Settings**¹.
6. Change **External Account Control** to **Enable**.
7. Select **Enable Authentication by External Server**.
8. Enter **SafeCom Go Sharp** in **Application Name**.
9. In **Address for Application UI**, enter the reference to a specific file on the connected SafeCom Controller. The address is:
http://<ip address>/soapsharp/safecom.scx
where <ip address> should be replaced with the IP address of the SafeCom Controller.
10. In **Address for Web Service**, enter the reference to a specific folder on the connected SafeCom Controller. The address is:
http://<ip address>/soapsharp/
where <ip address> should be replaced with the IP address of the SafeCom Controller.
11. Leave **Timeout** on 20 seconds.
12. Click **Submit**.
13. Do one of the following:
 - If **Standard Application Settings**² appears in the menu just above **External Accounting Application Settings** click **Reboot Later** and go to step 14.
 - Otherwise, click **Reboot Now** if you have completed the configuration and wait for the Sharp MFP to restart.

 If the web page reports "ERROR[5000]: Processing is in motion", press the **COPY** button on the Sharp MFP to bring it into copy mode, then click **Reboot Now** again.

14. Click **Standard Application Settings**².
15. Check if **Pull Print** is added:
 - If SafeCom Go Sharp has been enabled, **Pull Print** will appear among the listed applications.
 - If Pull Print does not appear, click **Add**. Otherwise, click **Pull Print** to see the configuration.
16. Enter **Pull Print** in **Application Name**.
17. Enter the reference to a specific file on the connected SafeCom Controller in **Address for Application UI**. The address is:
http://<ip address>/soapsharp/pullprint.scx
where <ip address> should be replaced with the IP address of the SafeCom Controller.
18. Leave **Timeout** on 20 seconds.
19. Click **Submit**.
20. Click **Reboot Now** and wait for the Sharp MFP to restart.

¹ **External Accounting Application Settings** menu item appears only if you have purchased the Sharp External Account Module (MX-AMX3), which is a prerequisite for SafeCom Go Sharp. If you install MX-AMX3 with full license, it disables the trial license.

² **Standard Application Settings** menu item appears only if you have purchased the Sharp Application Communication Module (MX-AMX2) and installed the license key. If you install MX-AMX2 with full license, it disables the trial license.

i f the web page reports "ERROR[5000]: Processing is in motion", press the **COPY** button on the Sharp MFP to bring it into copy mode, then click **Reboot Now** again.

Sharp Web Interface (old models)

Follow the steps below to configure the web interface on old Sharp devices. If you have a new Sharp device, see [Configure new Sharp devices](#).

The web interface must be configured to allow communication with the SafeCom Go Sharp solution.

1. Open the Sharp device's web interface and login.
2. Scroll to and click **Admin Mode**.
3. Enter the **User name** (default is admin) and **Password** (default is Sharp).
On newer models the default password is admin.
4. Click **OK**.
5. Scroll to and click **External Applications**.
6. Click **External Accounting**³.
7. Change **External Account Control** to **Enable**.
8. Select **Enable Authentication by External Server**.
9. In **Application Name**, enter **SafeCom Go Sharp**.
10. In **Address for Application UI**, enter the reference to a specific file on the connected SafeCom Controller. The address is:
http://<ip address>/soapsharp/safecom.scx
where <ip address> should be replaced with the IP address of the SafeCom Controller.
11. In **Address for Application Web Service**, enter the reference to a specific folder on the connected SafeCom Controller. The address is:
http://<ip address>/soapsharp/
where <ip address> should be replaced with the IP address of the SafeCom Controller.
12. Leave **Timeout** on 20 seconds.
13. Click **Submit**.
14. If **Standard Applications**⁴ appears as a link go to step 15. Otherwise, power down and restart the Sharp MFP.
15. Click **Standard Applications**.
16. If SafeCom Go Sharp has been enabled, **Pull Print** will appear among the listed applications.
 - If **Pull Print** does not appear then click **Add**.
 - Otherwise, select **Pull Print** and click **Edit** to see the configuration.
17. In **Application Name**, enter **Pull Print**.

³ **External Accounting** link appears only if you have purchased the Sharp Sharp External Account Module (MX-AMX3). This module is a prerequisite for SafeCom Go Sharp.


⁴ **Standard Applications** link appears only if you have purchased the Sharp Application Communication Module (MX-AMX2) and installed the license key.

18. In **Address for Application UI**, enter the reference to a specific file on the connected SafeCom Controller. The address is:
http://<ip address>/soapsharp/pullprint.scx
where <ip address> should be replaced with the IP address of the SafeCom Controller.
19. Leave **Timeout** on 20 seconds.
20. Click **Submit**.
21. Power down and restart the Sharp MFP.

Configure the SafeCom Controller Web Interface

Log in to the SafeCom Controller Web Interface

1. Open a web browser and enter the IP address of the SafeCom Controller in the address field. JavaScript (Active Scripting) must be enabled.
2. Click **Advanced Configuration** to open the **Advanced Configuration** web page.

 If a password is set you will be prompted for the password.

Advanced Configuration web page

The **Advanced Configuration** web page can be accessed from the link on the SafeCom Controller opening page. If the page is password-protected you will be prompted for a user name and password.



SafeCom web page

The **SafeCom** web page can be opened from the **Advanced Configuration** web page by clicking on **SafeCom**.

The screenshot displays the 'SafeCom Settings' page in the SafeCom Controller Administration interface. The page includes a navigation menu at the top with links for Home, Advanced Configuration, Status, How To, Technical Support, and Overview. The main content area is divided into two sections: 'SafeCom Settings' and 'Summary'.

SafeCom Settings:

- SafeCom Group Name:** WSLEJ3
- SafeCom Server IP Address:** 172.16.6.58 (with a note: 'Write one server per line. Highest priority on top. Example: 192.168.1.5')
- SafeCom Server Port Number:** 7500
- Broadcast Subnets:** 255.255.255.255 (with a note: 'Write one subnet per line. Example: 255.255.255.255')
- Front End Language:** English
- Front End Identification:** CODE_CARD
- Front End Timeout:** 60 (min 30 max 300 seconds)

Summary:

- SafeCom Controller Name:** SafeCom Controller 2 Port
- Contact:** Port
- Location:** S80 506.790*42
- Firmware:** S80 506.790*42
- Ethernet MAC Address:** 00C076FF1403
- IP Address:** 172.16.6.100

At the bottom of the settings section, there is a 'Save & Continue' button and a breadcrumb trail: 'SafeCom Controller Administration'.

SafeCom Group Name, SafeCom Server Address and **SafeCom Server Port Number** must be specified for the SafeCom Controller to work.

You can specify multiple SafeCom servers for the purpose of failover. The SafeCom Controller will attempt to contact the servers in their order of appearance.

If the IP Address is 0.0.0.0 the SafeCom Controller will send a broadcast on the **Broadcast subnets**.

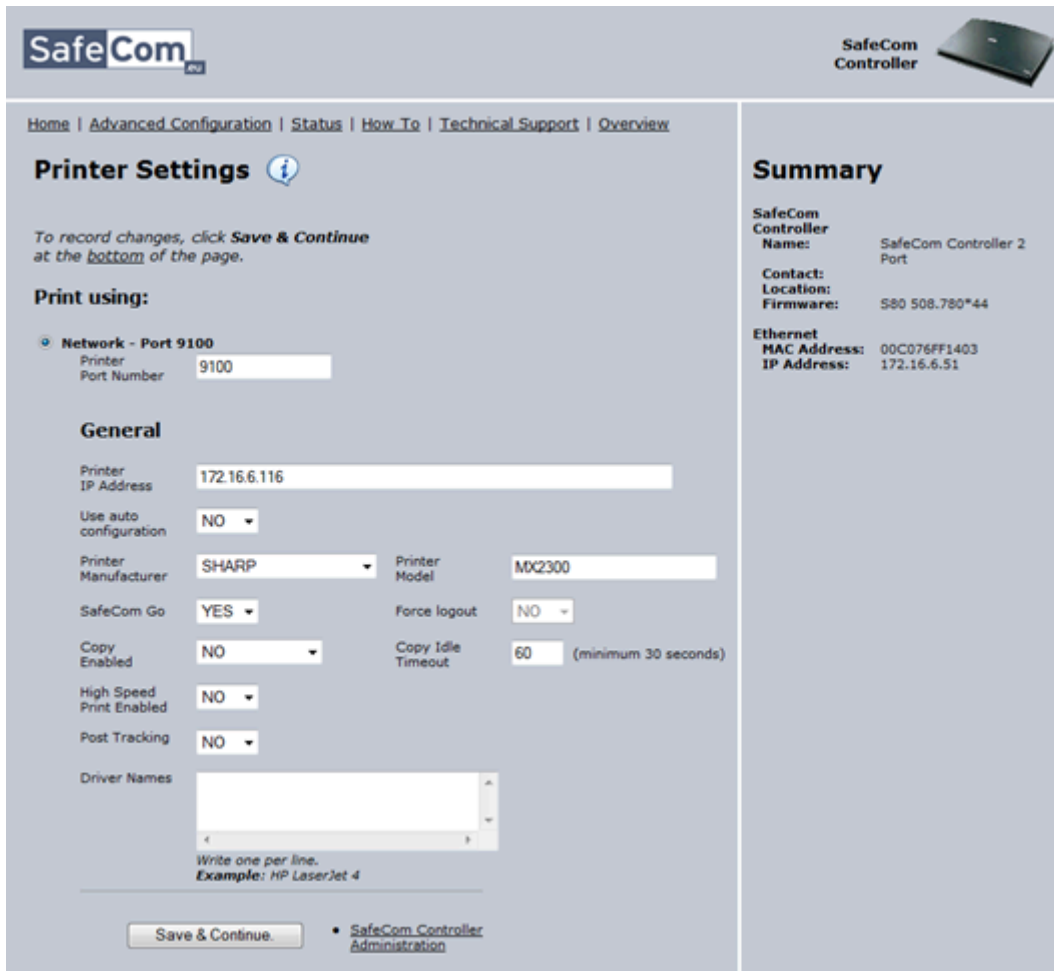
Front End Language: The supported language is English.

Front End Identification determines how users are identified. It can be **CODE_CARD** (default), **CODE_CARD** or **Windows_Auth**. The latter allows users to login with Windows user logon and Windows password.

The **Front End Timeout** default value is 60 seconds. Users will be logged out if they do not perform an operation on the Sharp MFP's touchscreen or buttons for this period.

Printer web page

The **Printer** web page can be opened from the **Advanced Configuration** web page by clicking on **Printer**.



Select **Network – Port 9100** if the SafeCom Controller connects to the device through the network.

Printer IP Address value must be that of the Sharp MFP.

Use auto-configuration value should normally be set to **YES** allow the SafeCom Controller to automatically determine the **Printer Manufacturer** and **Print Model**.

Printer Manufacturer value should be SHARP.

SafeCom Go value must be **YES**.

Copy Enabled value must be **YES** if you wish SafeCom to track the number of copies. Requires a SafeCom Tracking device license.

Copy Idle Timeout value is ignored.

High Speed Print Enabled value should be **YES** to allow faster printing. With high speed print, the print speed becomes comparable to that of printing the document directly to the device. High Speed Print works without any drawbacks in environments where users are only Pull Printing.

i With High Speed Print enabled, Push prints are deleted if they arrive at the device while a user is logged in.

Post Tracking will cause tracking data to be adjusted to reflect the actual number of mono and color pages printed.

i When Post Tracking is enabled and a user is logged in at the MFP, all jobs that are sent directly to the Sharp MFP are deleted.

Drivers: When Pull Printing, SafeCom will compare the driver name embedded in the print job with its list of driver names. If no match is found the document will appear with a question mark [?] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.

SafeCom Go for Controller - How to

Enable copy tracking for Controller

Copy tracking is disabled by default. To enable it, follow these steps:

1. Open the **Printer** web page.
2. Change **Copy Enabled** to **YES**.
3. Click **Save and Continue**.
4. Click **Restart**.

i Copy jobs are only tracked if the SafeCom license includes SafeCom Tracking. See also in [Copy jobs are not tracked](#).


Specify SafeCom Server and device connection

1. Open the **Advanced Configuration** web page.
2. Click **SafeCom** ([SafeCom web page](#)) and enter the **SafeCom Server address** (Hostname or IP address).
It is possible to specify multiple SafeCom servers for the purpose of failover. The SafeCom Controller will attempt to contact the servers in their order of appearance. If the SafeCom server is clustered you must specify the address of the virtual server.
3. Click **Save and Continue**.
4. Click **Printer** and select **Network - Port 9100**.
5. Enter the **Printer IP address**.
6. Click **Save and Continue**.
7. Click **Restart**.

After approximately 1 minute the SafeCom Controller has restarted and you can make a setting printout.

Register device


The device is registered when a user with Technician or Administrator rights has logged in at the device. Once the device is registered it will appear in the SafeCom Administrator. The device is also registered when you add it in SafeCom Administrator.

 You can use the built-in Technician account TECH with the default PUK code 12345678 and default PIN code 1234.

Set password to prevent unauthorized access

To prevent unauthorized access to the SafeCom Controller's configuration, we recommend that you change the password from the default: adm. To disable security, change the password back to adm.

1. Open the **Advanced Configuration** web page.
2. Click **Password**.
3. Enter the **Old Password**, **New Password** and **Verify Password**.
The password can be maximum 8 characters.
4. Click **Save and Continue**.
5. Click **Restart**.

 Make sure to store the password in a secure place. If you forget the password you need to return the SafeCom Controller to SafeCom for unlocking.

Assign a fixed IP address to the SafeCom Controller

The IP address can be assigned through DHCP (dynamic or fixed) or manually. The steps below describe how to assign a fixed IP address through the SafeCom Controller web interface.

1. Open the **Advanced Configuration** web page.
2. Click **TCP/IP**.
3. Select **Manual** and enter the **IP address** and other parameters.
4. Click **Save and Continue**.
5. Click **Restart**.

Select user identification

1. Open the **Advanced Configuration** web page.
2. Click **SafeCom**. Change **Front End Identification**.
3. Click **Save and Continue** to save your settings.
4. Select **Restart**. Click **Restart** again.

You must wait approximately 1 minute while SafeCom initializes. If the control panel on the Sharp MFP does not reflect the change in the login screen, refresh the screen by pressing the JOB STATUS button on the Sharp MFP, then press the COPY button.

Disable the Test button

To prevent unauthorized users from restoring factory default you can disable the SafeCom Controller's test button.


1. Open the **Advanced Configuration** web page.
2. Click **General**.
3. Change **Enable Test Button** to **NO**.
4. Click **Save and Continue**.
5. Click **Restart**.

Enable Copy Control

1. Open the **Advanced Configuration** web page.
2. Click **Printer** and change **Copy Enabled** to **YES**.
3. Change **Use auto** configuration to **YES**.
4. Click **Save and Continue**.
5. Click **Restart**.

Enable High Speed Print

1. Open the **Advanced Configuration** web page.
2. Click **Printer** and change **High Speed Print Enabled** to **YES** if print data needs to be sent directly and unencrypted to the device from the SafeCom server rather than through the SafeCom Controller.

 If the document is sent encrypted to the device, the High Speed Print is ignored.

3. Click **Save and Continue**.
4. Click **Restart**.

Access Sharp MFP's System Settings

1. Log in at the Sharp MFP as a user with administrator or technician rights in SafeCom.
2. Press the **COPY** button to get into copy mode.
3. Press the **SYSTEM SETTINGS** button to access the Sharp MFP's system settings.

Restore factory default

You can either restore settings by holding down the test button of the SafeCom Controller for 8 seconds, or from the SafeCom Controller web interface:

1. Open the **Advanced Configuration** web page.


2. Click **Restore Factory Default**.

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 the 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**.

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

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

Uninstall SafeCom Go Sharp

1. Open the Sharp MFP's web page and login.
2. Click **Application Settings > External Applications Settings**.
3. If there is no **Standard Application Settings**⁵ menu item go to step 6.
4. Click **Standard Application Settings**.
5. Select **Pull Print** and click **Delete**.
6. Click **External Accounting Application Settings**.
7. Change **External Account Control** to **Disable**.
8. Click **Submit**.
9. Click **Reboot Now** and wait for the Sharp MFP to restart.

 If the web page reports "ERROR[5000]: Processing is in motion" press the **COPY** button on the Sharp MFP to bring it into copy mode and then click **Reboot Now** again.

10. Restore the SafeCom Controller to factory defaults.

⁵ **Standard Application Settings** menu item appears only if you have purchased the Sharp Application Communication Module (MX-AMX2) and installed the license key.

Chapter 5

Using SafeCom Go Sharp

Sharp device with SafeCom Device Server

Login

The different login sequences are described in the section. The welcome screen is enabled by default, but if it is disabled the user is guided directly to the login sequence.

Log in with card

1. Tap the **Login** icon.
2. Use the card reader.

Log in with card and PIN code

1. Tap the **Login** icon.
2. Use the card reader.
3. Enter **PIN code** using the touchscreen or keypad.
4. Tap **OK**.

Log in with ID code

1. Tap the **Login** icon.
2. Enter the **ID code** using the touchscreen or keypad.
3. Tap **OK**.


Log in with ID code and PIN code

1. Tap the **Login** icon.
2. Enter the **ID code** using the touchscreen or keypad.
3. Tap **OK**.
4. Enter **PIN code** on the touchscreen.
5. Tap **OK**.

Log in with Windows

1. Tap the **Windows login** icon.
2. Tap **Username** and enter **Username** on the touchscreen.

3. Tap **OK**.
4. Tap **Password** and enter **Password** on the touchscreen.
5. Tap **OK**.
6. If domain is required, tap the **Domain** drop-down list and select domain.
7. Tap **OK**.

 Username and password cannot be blank.

Main menu

Once logged in you can select an option from the touchscreen.

Perform one of the following actions:

- Tap **Pull Print** to print individual documents.
- Tap **Copy / Scan** to start copy or scan.
- Tap **Account** to select billing code.
- Tap **Log out** to log out.

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.



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 (newest 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 **Back** to return to the main screen.
- Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.

Copy

1. Tap **Copy / Scan** in the login screen to start copy or scan.
2. Press the **COPY** button on the Sharp MFP to bring it into copy mode.
3. Press the **Start** button to copy the documents placed in the automatic document feeder (ADF).
On some Sharp MFPs there are two **Start** buttons - one for black/white copies and one for color copies.




- Once logged in to the Copy/Scan function, the user cannot change to Pull Print unless the users logs out and logs in again. This is due to restrictions in the Sharp MFP. Purchasing the Sharp Application Communication Module (MX-AMX2) removes this restriction.
- When a pay user begins copying, SafeCom Go Sharp uses the charging scheme to calculate the equivalent number of mono A4 simplex pages the user can copy with the available credits. If the user instead copies for example, A3 color pages, the user can run into negative balance. Pages are counted as they are printed and hence there may be an overrun of 4-8 pages.
- On Sharp AR-MXXX models, SafeCom Pay is not recommended as there are no means to stop the copy process when the user runs out of credits.

Account – Select billing code

1. Tap the **Account** icon to select a billing code.
2. Tap **Favorites** to select from the list of the user's favorite billing codes.
They are listed in alphabetical order.
3. Tap **Last used** to select from the list of up to 10 of the user's last used billing codes.
The last used code is at the top of the list.
4. Continue by selecting one of the following options:
 - Tap **Billable** to use the selected billing code.

- Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
 - Tap **Personal** to return to the home screen without selecting a billing code. When selecting Personal, the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.
 - Tap **Info** to see information about the selected billing code, including the unabbreviated description.
5. Finish the job at the device.

 Whether or not the user has the options to work with billing codes when printing depends on how the **User properties** and the **Device Properties** are set up in **SafeCom Administrator**. The user must have **Bill clients for cost** selected on the **Settings** tab, and the **Client Billing** must be selected on the **License** tab on the **Device properties**. If client billing is set up correctly in the user properties, but not in the **Device properties**, the client billing user is able to select the **Account** icon on the device, but there will be no billing codes to work with.

Register card

The user logs in by entering an ID code or using a card. If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is asked to enter his PUK code.

Enter PUK code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **OK**.

Enter PUK code and PIN code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **PIN code**.
5. Enter **PIN code** on the touchscreen.
6. Tap **OK**.
7. Tap **OK**.

Enter Windows credentials

1. Use the card at the device's card reader and tap **OK**.
2. If prompted for a PUK code, tap **Windows Login** and a prompt for Windows credentials opens.
3. Tap the **Username** field and enter the user name using the keypad or touchscreen.

4. Tap the **Password** field and enter the password.
5. Tap the **Domain** field and enter the domain.
6. Tap **OK**. To cancel card registration tap **Cancel**.

Logout

There is a configurable Timeout that has a default value of 30 seconds. The logout process is initiated if no buttons are tapped for this period.

Tap **Log out** on the main screen.

Sharp MX devices with MX-AMX2 license

Login

The different login sequences are described in the following section. The Welcome screen is enabled by default ([Configure device in SafeCom Device Server](#)), but if it is disabled the user is guided directly to the login sequence.

Log in with card

1. Tap the **Login** icon.
2. Use the card reader.

Log in with card and PIN code

1. Tap the **Login** icon.
2. Use the card reader.
3. Enter **PIN code** using the touchscreen or keypad.
4. Tap **OK**.

Log in with ID code

1. Tap the **Login** icon.
2. Enter the **ID code** using the touchscreen or keypad.
3. Tap **OK**.

Log in with ID code and PIN code

1. Tap the **Login** icon.
2. Enter the **ID code** using the touchscreen or keypad.
3. Tap **OK**.
4. Enter **PIN code** on the touchscreen.
5. Tap **OK**.

Log in with Windows

1. Tap the **Windows login** icon.
2. Tap **Username** and enter **Username** on the touchscreen
3. Tap **OK**.
4. Tap **Password** and enter **Password** on the touchscreen.
5. Tap **OK**.
6. If domain is required, tap the **Domain** drop-down list and select domain.
7. Tap **OK**.



- Username and password cannot be blank.
- Due to device limitations, the Windows password is not masked while typing on MX-2600N devices.

Main menu

Once logged in you can select an option from the touchscreen.

Perform any of the following actions:

- Tap **Pull Print** to print individual documents.
- Tap **Copy / Scan** to start copy or scan.
- Tap **Account** to select billing code.
- Tap **Log out** to log out.

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.

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 (newest 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 **Back** to return to the main screen.


- Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.

Copy

1. Tap **Copy / Scan** in the login screen to start copy or scan.
2. Press the **COPY** button on the MFP to bring it into copy mode.
3. Press the **Start** button to copy the documents placed in the automatic document feeder (ADF).
On some MFPs there are two **Start** buttons - one for black/white copies and one for color copies.

Account – Select billing code

1. Tap the **Account** icon to select a billing code.
2. Tap **Favorites** to select from the list of the user's favorite billing codes.
They are listed in alphabetical order.
3. Tap **Last used** to select from the list of up to 10 of the user's last used billing codes.
The last used code is at the top of the list.
4. Continue by selecting one of the following options:
 - Tap **Billable** to use the selected billing code.
 - Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
 - Tap **Personal** to return to the home screen without selecting a billing code. When selecting **Personal**, the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.
 - Tap **Info** to see information about the selected billing code, including the unabbreviated description.
5. Finish the job at the device.

 Whether or not the user has the options to work with billing codes when printing depends on how the **User properties** and the **Device Properties** are set up in **SafeCom Administrator**. The user must have **Bill clients for cost** selected on the **Settings** tab, and **Client Billing** must be selected on the **License** tab on the **Device properties**. If client billing is set up correctly in the user properties, but not in the **Device properties**, the client billing user is able to select the **Account** icon on the device, but there will be no billing codes to work with.

Register card

The user logs in by entering an ID code or using a card. If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is asked to enter his PUK code.

Enter PUK code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **OK**.

Enter PUK code and PIN code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **PIN code**.
5. Enter **PIN code** on the touchscreen.
6. Tap **OK**.
7. Tap **OK**.

Enter Windows credentials

1. Use the card at the device's card reader and tap **OK**.
2. If prompted for a PUK code, tap **Windows Login**.
A prompt for Windows credentials opens.
3. Tap the **Username** field and enter the user name using the keypad or touchscreen.
4. Tap the **Password** field and enter the password.
5. Tap the **Domain** field and enter the domain.
6. Tap **OK**. To cancel card registration tap **Cancel**.

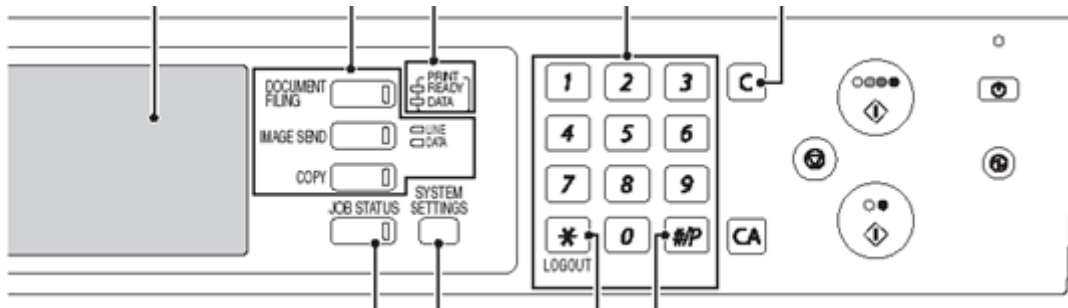
Logout

There is a configurable Timeout that has a default value of 30 seconds. The logout process is initiated if no buttons are tapped for this period.

Tap **Log out** on the main screen.

Sharp device with SafeCom Controller

Control panel



Login

The different login sequences are described in the following section.

Log in with card

Use the card reader.

Log in with card and PIN code

1. Use the card reader.
2. Enter **PIN code** using the touchscreen.
3. Tap **OK**.
4. Tap **OK**.

Log in with ID code

1. Tap **ID code**.
2. Enter the **ID code** using the touchscreen.
3. Tap **OK**.
4. Tap **OK**.


Log in with ID code and PIN code

1. Tap **ID code**.
2. Enter the **ID code** using the touchscreen.
3. Tap **OK**.
4. Enter **PIN code** on the touchscreen.
5. Tap **OK**.
6. Tap **OK**.

Log in with Windows

If Front End Identification is Windows_Auth, it is possible to login by either using your card or entering your Windows login credentials:

1. Tap **Username** and enter **Username** on the touchscreen.
2. Tap **OK**.
3. Tap **Password** and enter **Password** on the touchscreen.
4. Tap **OK**.
5. Tap **OK**.

 Username and password cannot be blank.

Main menu

Once logged in you can select an option from the touchscreen. Tap **Print All** to print all documents except the retained documents. Documents are printed in chronological order (oldest first).

Perform any of the following actions:

- Tap **Documents** to print individual documents.
- Tap **Copy / Scan** to start copy or scan.
- Tap **Settings** to see the settings.
- Tap **Log out** to log out.

Pull Print - Document list

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

Tap **Documents**.

Documents appear in chronological order with the newest at the top of the list.

The preceding **R** shows the document is retained. The number is the cost of the document. 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 (newest 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 **Back** to return to the main screen.
- Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.

Copy

1. If Copy Control is disabled tap **Copy / Scan** in the login screen to start copy or scan. If Copy Control is enabled you have to login first and then tap **Copy / Scan** to start copy or scan.
2. Press the **COPY** button on the MFP to bring it into copy mode.
3. Press the **Start** button to copy the documents placed in the automatic document feeder (ADF).



- Once logged in to the Copy/Scan function the user cannot change to Pull Print, unless the users logs out and logs in again. This is due to restrictions in the Sharp MFP. Purchasing the Sharp Application Communication Module (MX-AMX2) removes this restriction.
- When a pay user begins copying, SafeCom Go Sharp uses the charging scheme to calculate the equivalent number of mono A4 simplex pages the user can copy with the available credits. If the user instead copies for example, A3 color pages, the user can run into negative balance. Pages are counted as they are printed and hence there may be an overrun of 4-8 pages.
- On Sharp AR-MXXX models SafeCom Pay is not recommended as there are no means to stop the copy process when the user runs out of credits.

Register card with PUK code

The user goes to the device to login by entering an ID code or using a card. If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.

Enter PUK code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **OK**.

Enter PUK code and PIN code

1. Tap **PUK code**.
2. Enter **PUK code** on the touchscreen.
3. Tap **OK**.
4. Tap **PIN code**.
5. Enter **PIN code** on the touchscreen.
6. Tap **OK**.
7. Tap **OK**.

Logout

There is a configurable Timeout that has a default value of 30 seconds. The logout process is initiated if no buttons are tapped for this period.

Do one of the following:

- Tap **Log Out** on the main screen.
- Use the card, if user logged in with card.

Chapter 6

Troubleshooting

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`

i 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 Administrator: Unable to locate all SafeCom devices

1. In **SafeCom Administrator** click on the **Preferences > Options**, and verify that the list of **Broadcasts addresses** on the **Network** tab is correct.
2. Check that the LAN LED on the front of the SafeCom Controller is solid on as this indicates that it has an IP address.
3. Contact a network administrator that has access to the DHCP server.
4. Obtain the SafeCom Controller's MAC address.
The MAC address is printed on the white label on the bottom of the SafeCom Controller. It is a 12-digit hexadecimal number, for example: 00C076FF00F2. The network administrator can login to the DHCP server and see the IP address that is assigned to the SafeCom Controller.
5. Once you have the IP address click **Add device...** in **SafeCom Administrator**.

Copy jobs are not tracked

Check the following:

- **Copy Enabled** is **YES** on the SafeCom Controller's **Printer** web page.
- **Tracking** is selected on the **License** tab in the **Device properties** dialog box of the **SafeCom Administrator**.
- Cost control is set to **Tracking** or **Pay** on the **Settings** tab in the **User properties** dialog box in **SafeCom Administrator**.

Print performance is slow

Print performance can be improved when printing large files by enabling High Speed Print.

At the printer: No billing codes available

If there are no billing codes available for the user logged in to the device, select the set up of User properties and Device properties in the SafeCom Administrator.

Make sure that the following settings are correct:

- In **User properties** > **Settings** tab, **Bill clients for cost** must be selected.
- In **Device properties** > **License** tab, the **Client Billing** must be selected.

If client billing is set up correctly in the User properties, but not in the Device properties, the client billing user is able to select the Account icon on the device, but there will be no billing codes to work with.

MFP reports: Could not access the accounting server...

The touchscreen on the Sharp MFP reports "Could not access accounting server. Contact your administrator".

Check the following:

- Verify that the SafeCom Controller is powered on, network connected and working.
- Verify that Sharp web interface is configured with the IP address of the connected SafeCom Controller.
- Ensure that the **Offline mode** of the Sharp MFP is set to **Disabled**.

ERROR[5000]: Processing is in motion

If the Sharp web page reports "ERROR[5000]: Processing is in motion", press the COPY button on the Sharp MFP to bring it into copy mode and then click Reboot Now again.

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"

Complete these steps 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 with the following command:

```
net start scDeviceServer
```
4. Re-run the SafeCom Device Server installer.

Device Server: Pull Print icon is not available

Check the following:

- If you cannot see the Pull Print icon on a device you added to your Device Server, ensure that the link to the Pull Print application is correct. To do so, open the device web page, browse to **Application Settings > External Applications Settings > Standard Application Settings** and

ensure that Pull Print is named correctly, and the **Address for Application UI** field displays the correct address (<http://<Safecom Device server ip-address>:8080/safecomosa/PullPrintScreen>).

- If needed, check the availability of the Account icon similarly. Ensure that the **BillingEnabled** property of the device is set to **True** through the Device Server. On the device webpage, browse to **Application Settings > External Applications Settings > External Accounting Application Settings** and ensure that all settings are correctly enabled, and the address field displays (<https://<Safecom Device server ip-address>:50002/safecomosa/BillingScreen>).

SafeCom reader does not work

If the SafeCom reader does not work, the below settings must be checked and set by a Sharp Technician:

```
Sim55-3 SW 5  
Bit 1 2 3 4 5 6 7 8  
Data 1 1 1 0 0 0 0 1
```

User auto logout does not work when the device goes to sleep on some Sharp devices

Ensure that the Auto Clear Setting timer is lower than the Auto Power Shut-Off timer.

Chapter 7

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.