Kofax SafeCom Go Sharp

Administrator's Guide

Version: 9.12.0

Date: 2020-12-11

KOFAX

Table of Contents

Preface

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

Related documentation

The full documentation set for Kofax SafeCom Go Sharp is available at the following location https://docshield.kofax.com/Portal/Products/SafeCom/10.530-jaah72kksf/SafeCom.htm

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

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

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

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

Training

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

Getting help for Kofax products

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

To access the Kofax Knowledge Base, go to the Kofax website and select Support on the home page.

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

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

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

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

Introduction

SafeCom Go Sharp

SafeCom Go Sharp is the embedded solution for Sharp MFPs. It integrates with the touch-screen 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** (2)
  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** (3)
  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

Table 1 SafeCom Go Sharp supported SafeCom ID Devices

Identification Method	USB	Serial	USB Keyboard
	SafeCom Controller		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

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

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

The Device Administrator user name and password is required to login:

Table 2 Sharp device passwords

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

SafeCom Go Sharp - Device server

Overview

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

SafeCom Go Sharp - Device server installation

Installation

1. Download the safecom_device_server_nnn.exe file from the link supplied to you. The installation must be **Run as administrator.**

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

2. When the installation program is launched click **Next**.
3. Choose the destination folder for the files. Click **Next**.

   The default installation folder is:

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

   On **Windows 64-bit**:

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

4. Click **Next**.
5. Review settings before copying of files starts. Click **Next**.
6. Click **Finish**.

Windows Firewall - Ports that must be opened

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

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

You can also manually ensure that the port numbers below are open.
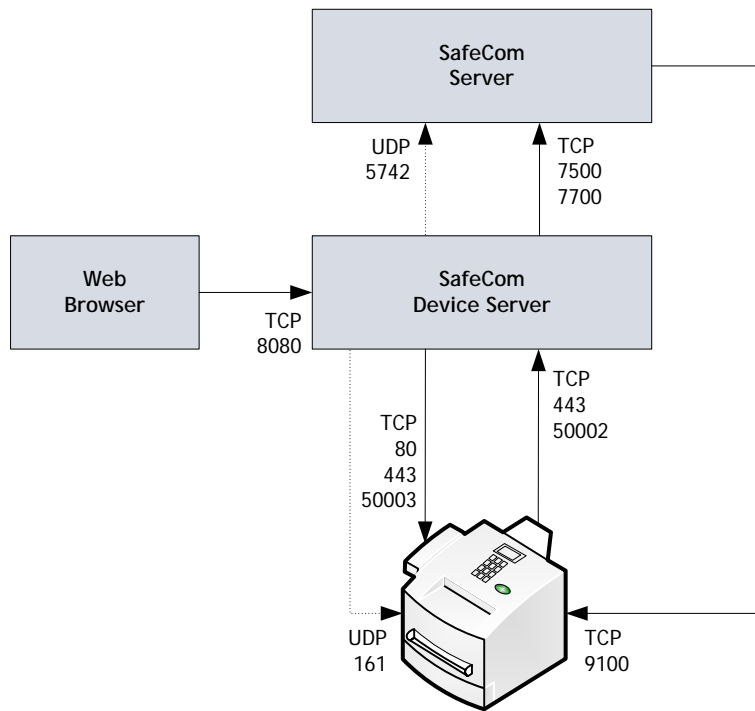
TCP	Inbound on SafeCom Device Server	Protocol
80	Used to contact MFP during initial setup	HTTP
443	Used to contact MFP during operation	HTTPS
8080	Web browser	HTTP
50002	Device	HTTPS
UDP	**Inbound on SafeCom Device Server**	**Protocol**
161	Used to register notifications	SNMP
TCP	**Outbound on SafeCom Device Server**	**Protocol**
443	Used to contact MFP during operation	HTTPS
7500	SafeCom Server (Job Server)	SafeCom
7700	SafeCom Server (Job Server)	SafeCom
50003	Device	HTTPS
UDP	**Outbound on SafeCom Device Server**	**Protocol**
5742	SafeCom Server (Broadcast Server)	SafeCom
TCP		**Protocol**
9100	Used for printing	RAW

Configure SafeCom Device Server

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

Login to SafeCom Device Server

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

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

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

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

Add SafeCom Server

1. Log in to **SafeCom Device Server**.
2. Click **Device Server** in the left pane.
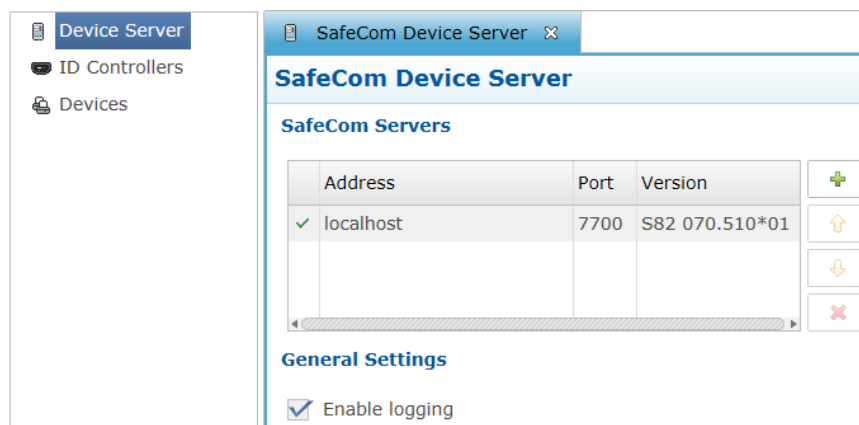
3. Under **SafeCom Servers**, click the **[+]** icon to add a failover SafeCom Server.
4. Enter the server address and click **OK**. To add localhost as the server, leave the **Address** field blank and click **OK**.
5. Click **Save**.

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

Device Server config.ini

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

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

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

Setting	Description	Default
`deviceserver.encryptconfig`	Defines if configuration file is encrypted: 'true'=enable, 'false'=disable.	true
`deviceserver.configuredevices`	Option to disable the configuration code against devices. Useful mostly for testing purposes to support simulated devices.	true
`deviceserver.trace`	If set to 'true' it enables the server trace files	false
`deviceserver.protocol.trace`	If 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 max 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 max size of each third party trace file. Defined in bytes but takes a postfix for larger units: KB, MB or GB. Set only if needed.	N/A
`deviceserver.thirdparty.trace.file.count`	Defines the number of third party trace files to keep. Set only if needed.	N/A

Add device to a SafeCom Device Server

The device can be added to the SafeCom Device Server using one of the following two methods:

- Via the SafeCom Device Server.
  Solutions based on SafeCom G2 must use this method.

- Via the SafeCom Administrator.
  This is the recommended method and it works for SafeCom G3 Server version S82 070.410*05 or newer.
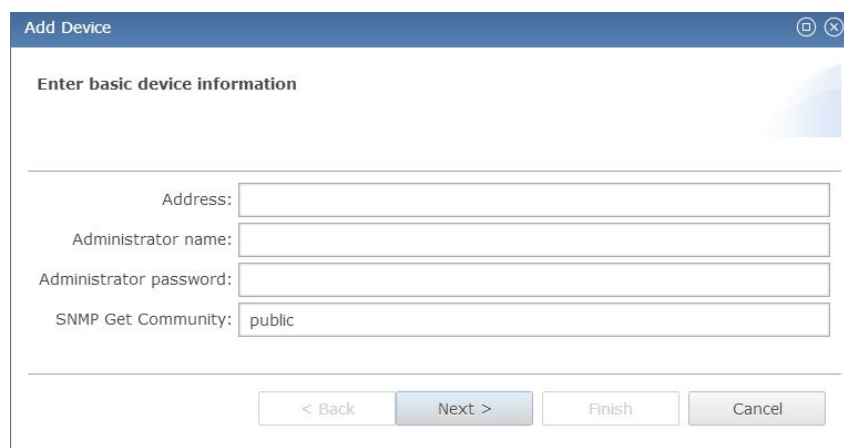
Device icons

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

User is logged in at the device.

Device is idle, no user logged in.

Wait for at least 2 minutes. If the warning signal is gone, the printer is now configured. If the warning signal remains, the printer cannot be configured because, for example the SSL is not on, or another device server is trying to configure the printer.

An error occurred.

The printer is receiving print data.

Device server cannot contact the printer.

Add device via SafeCom Device Server

1. Log in to **SafeCom Device Server**.
2. Click the **Add device** tool button.
3. Enter the hostname or the IP address of the device. If you want to use dynamic IP address, then enter the device hostname in the **Address** field. You can also set the SNMP community name of the device here.
4. Click **Next**.

5. Information is retrieved from the device to establish the type of device. Make the necessary adjustments to the **Required Device properties**.
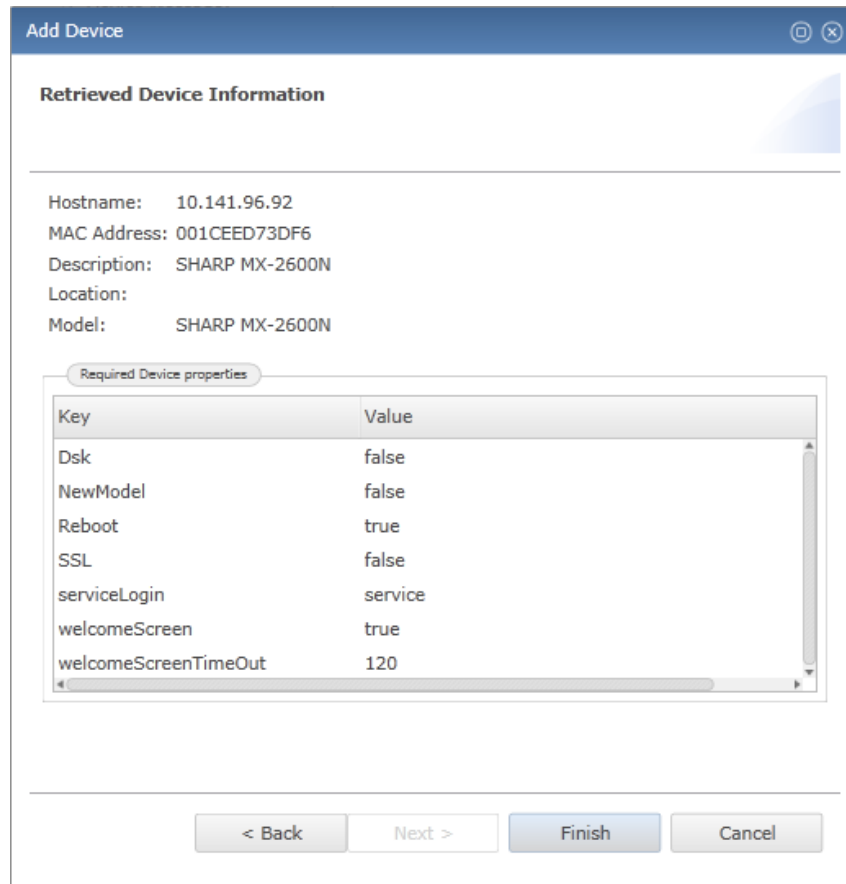
6. Click **Finish** and then **Save** 💾 and the device is now added to the SafeCom solution and will also appear in **SafeCom Administrator**.
7. On the device settings page, make sure the settings are correct.
8. Click **Save** 💾.

Add device via SafeCom Administrator

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

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

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

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

Add device server device

1. Click the **Devices** container, right-click the content area and then **Add device**. The **Add device wizard** is now launched.
2. From the **Device server** drop down menu, select the **SafeCom Device Server** and click **Next**.
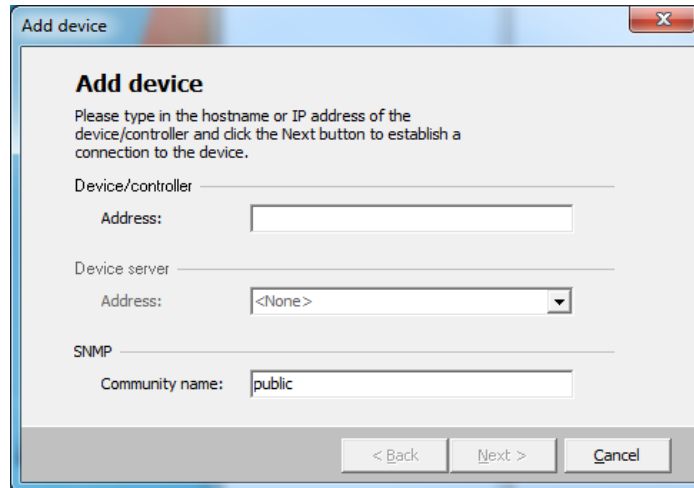
3. Information is retrieved from the device server to establish the status of device server. Click **Next**.
4. Enter the **Printer address** (the device IP address or host name) and click **Next**.
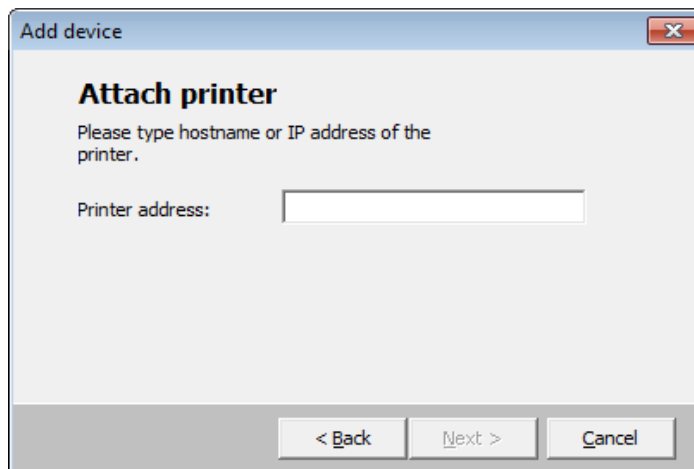
5. Information is then retrieved from the device. Click **Next**.
6. Now select **SafeCom Go Sharp** as the type of device and click **Next**.
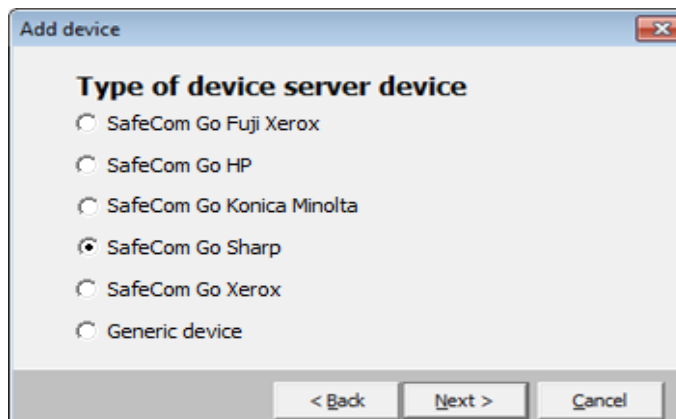
7. For the device enter the **User name** (default is admin) and **Password** (default is admin). On older devices the default password is Sharp.
8. The device properties dialog now opens. Make sure to specify on the **Settings** tab the device server and the capabilities of the device.

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

The device server device is now added and listed both under **Devices** and under the device server under **Device servers** with the name SafeCom Device Server.
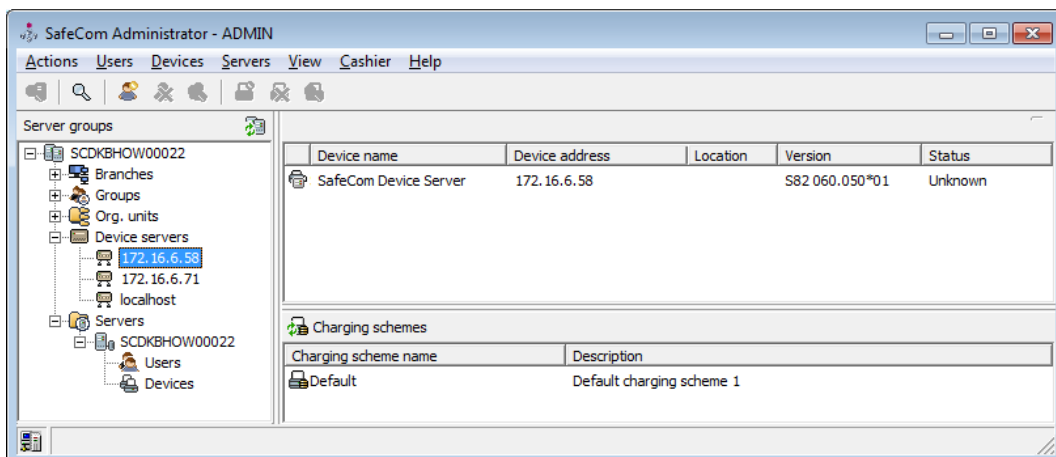
Configure device in SafeCom Device Server
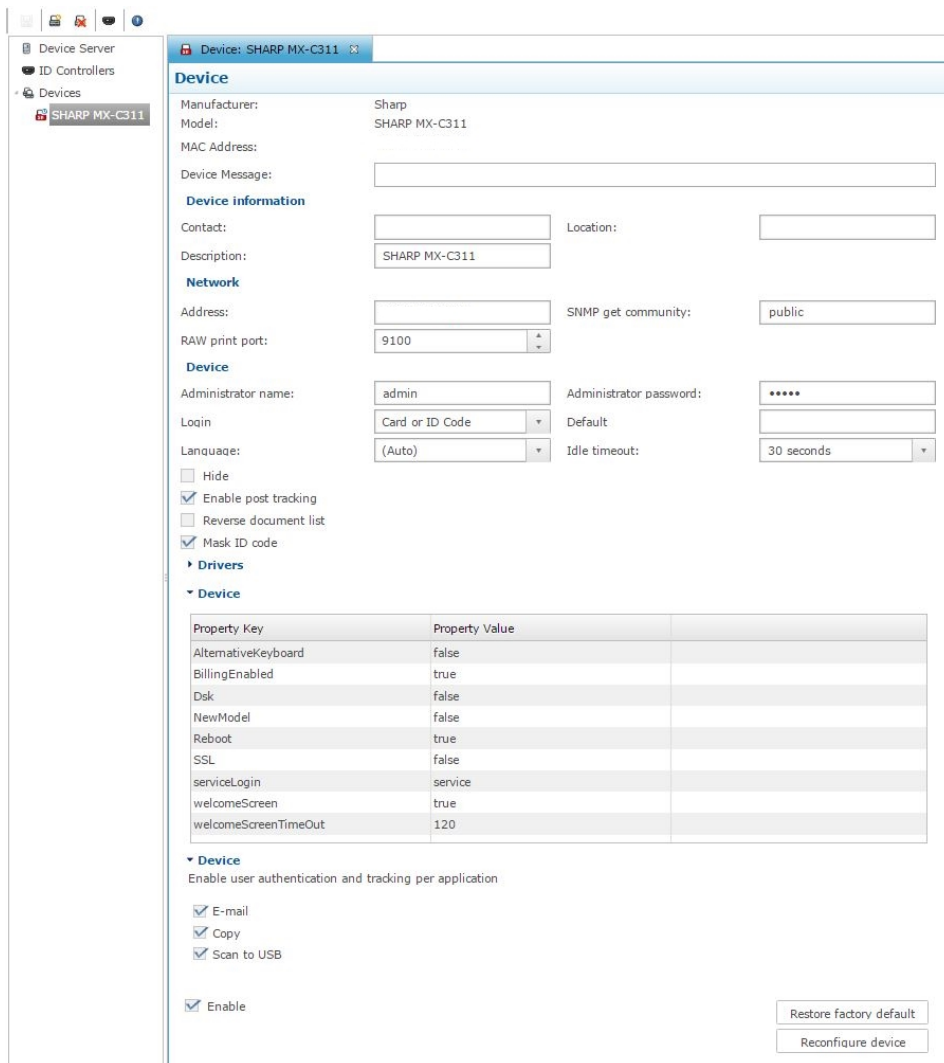
The **Device** tab is used to configure SafeCom Go Sharp with regards to which device it is connected to, how users are to be identified etc.

Note: If the configuration of the devices fails it might be because the Device Server is installed on a server that has multiple NICs or IPs. Refer to <u>Device Server: Configuration of devices failed</u> for a resolution.

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

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

Note 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:

- **Device information**
    - o **Manufacturer** and **Description** are automatically filled-in and together with **Location** they are also viewable in the **Device properties** dialog in **SafeCom Administrator**.
    - o **Contact** and **Location** provides useful information in maintaining the SafeCom solution.

- **Network settings**
    - o **Address:** The IP address of the device.
    - o **RAW print port:** The TCP port used to send print data.
    - o **SNMP Community name:** This must match the SNMP Community Name of the device. By default SNMP Community name is **public**.

- **Device settings**
    - o **Administrator name:** The user name with which the administrator can log in to device.
    - o **Administrator password (mandatory):** The device password with which the administrator can log in to device.
    - o **Login method:** This determines how users log in. Choose between:
        - – **Card**
        - – **ID code**
        - – **Card or ID code**
        - – **Card or Windows:** Allows the user to log in by either card or by typing in their Windows credentials and selecting domain from drop-down list.

        Note Identification by card requires connecting a USB ID Device (card reader). The option **Card or Windows** allows the user to log in by either card or by entering their Windows username, password, and domain. The SafeCom G4 server must be a member of the domain or trusted by the domain.

    - o **Default domain:** Specify the domain to pre-fill the domain for users when logging into a device. If using SafeCom Mobile Pull Print the domain must be specified, as the users are not prompted for domain when logging into a device using a smart phone. If the default domain is not specified, but the users are required to use domains, they can enter the domain with their username (domain\username).
    - o **Idle timeout:** Specifies in seconds when a logged in user is automatically logged out if there's no activity.
    - o **Hide domain:** Usable if you specified a default domain. Check to allow the users to log in without typing in the domain.
    - o **Enable post tracking:** This is relevant only with SafeCom Tracking. Refer to the *SafeCom G4 Administrator's Manual.*
    - o **Reverse document list:** Check to show the first printed documents at the top of the document list.
    - o **Mask ID code:** Check to mask the ID code with asterisk (*) when entered at the device.

- **Drivers**: When Pull Printing, SafeCom compares the driver name embedded in the print job with its list of driver names. If no match is found and if **Show fidelity warning** is checked in the **Server properties** in the **SafeCom Administrator**, the document appears with a question mark [?] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.
    - o Click **Get All** to obtain the list of drivers from the SafeCom Server or add and delete drivers manually.

- **Device Properties:**
  - o **DSK:** If the Device Security Kit is installed, **DSK** must be set to **True** and then the addresses for **Application UI** (`http://<Safecom Device server ip-address>:8080/safecomosa/go`) and **Web Service** (`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**.
  - o **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**.
  - o **Reboot:** Is set to **True**, which means that the device automatically restarts. Set to **False** if you want to restart the device manually.
  - o **SSL:** Set to **True** to use SSL.
  - o **AlternativeKeyboard:** Set to **True** to use the alternative keyboard. Use it if you encounter PIN/password masking issues due to the device display.
  - o **BillingEnabled:** Set to **True** to display the **Account** icon on the device screen, allowing to you set up the billable account. Set to **False** to remove the icon.

    Note If you set the BillingEnabled property on an already-configured device, you need to reconfigure the device for the change to take effect.

  - o **serviceLogin:** This service password must correspond to the service password on the device. The default is service.
  - o **welcomeScreen:** Set the property value to **True** if you want the welcome screen (see below) 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'.

    Note The property requires an AMX-3 license to work; devices with both AMX-2 and AMX-3 licenses do not display the screen set via this property.

  - o **welcomeScreenTimeOut:** Specify in seconds for when the welcome screen should timeout. The default value is '120'.
  - o **AlternativeKeyboard:** Set the property value to True to use an alternative virtual keyboard for masking sensitive information (ID, PIN, and so forth) on Sharp devices with older firmware. This may result in some rare language-specific characters being unavailable.

- **Device applications:** Here it is specified if the users are allowed to **Email**, **Copy**, or **Scan to USB** without having to log in first. Check one or more of the three checkboxes to allow the users to perform these tasks without authentication.

  The settings in the **Device applications** are tied to the welcome screen (see below). If one or more of the check boxes **Email**, **Copy**, or **Scan to USB** are selected, then the welcome screen only shows the option to **Login** and if enabled, **Windows login**. If none of the three checkboxes **Email**, **Copy**, or **Scan to USB** are selected the users have the option to **Login** and to **Copy/Scan** from the welcome screen.

- **Enable logging:** Select if log information should be collected.

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

- **Restore factory default** sets all settings, except the password, to their default value (refer to <u>Restore factory default</u>).
- **Reconfigure device** informs the device to reference the current SafeCom Device Server.

SafeCom Go Sharp - How to

The following subsections 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 left-hand menu, and then click on the device.
3. In the **Login method** drop down menu under **SafeCom Settings**, select how users must identify themselves at the device.

    Choose between:
    - ID code
    - Card
    - Card or ID code (default)
    - Card or Windows

Note When changing login method from Card or Id code to Card or Windows the change will take effect upon having logged 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 login to the SafeCom Device Server.
2. Click on **Device server** in the left-hand menu, and then click on the device.
3. Click **Device applications.**
4. Check **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 login to the SafeCom Device Server.
2. Click on **Device server** in the left-hand menu, and then click on the device.
3. Click **Device applications.**
4. Check **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 via SafeCom Administrator, refer to the *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

Note 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

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

For details on how to print a QR code for the device, refer to the *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 (domain\username).

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

Restore factory default

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

The factory default values are:

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		
Device properties	welcomeScreen	
	welcomeScreenTimeOut	120
	adminLogin	admin
	adminUserName	admin
	serviceLogin	service
	NewModel	false
		Date and time of configuration
Device applications	E-mail	Checked (Yes)
	Pull Print	Checked (Yes)
	Copy	Checked (Yes)
	Scan to USB	Checked (Yes)
Logging	Enable logging	Checked (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**.

> **Note** 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 login to the **SafeCom Device Server**.
2. Click **Device server** in the menu and select the device from which the SafeCom Go solution must be uninstalled.

3. Click the **Delete** icon in the top menu to uninstall.
4. Click **OK** to confirm deleting the SafeCom solution.

SafeCom Go Sharp device trace facility

Note Use the SafeCom trace facility only if SafeCom 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 checkbox **Logging enabled** at the bottom of the page is selected.
3. Click **Save**.

To see the trace files generated by the Device Server:

1. Go to the destination folder for the log files:

   The default installation folder is:

   ```
   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.

You can configure the size of the trace files as well as how many are generated.

1. Browse to the `config.ini` file:

   ```
   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 open 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.

SafeCom Controller

Installation with SafeCom Controller

1. Make sure the SafeCom G4 Server software installation has been completed as described in the *SafeCom Smart Printing Administrator's Quick Guide.*
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to 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. Refer to the device's manual.

IP address / hostname:
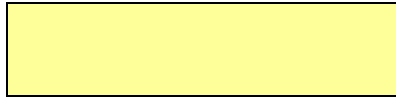
Note The SafeCom Controller MUST reference the Sharp device by a fixed IP address or a fixed fully qualified hostname. Example: mysharp.safecom.eu.

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.
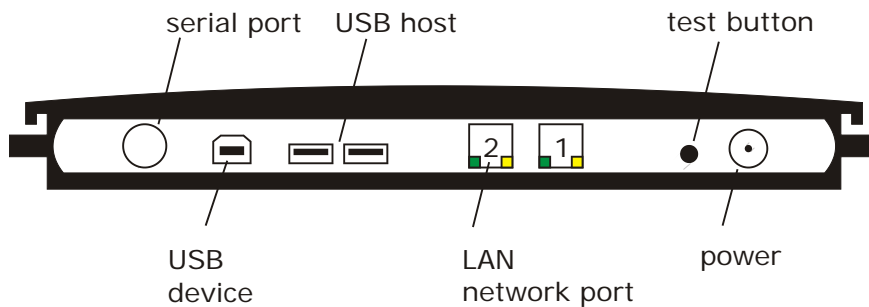
Figure 1 SafeCom Controller's rear panel

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 approx. 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. Next you need to determine the IP address of the SafeCom Controller so you can add it to the SafeCom solution.

- **Find IP address via 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. 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).

IP address known from DHCP server:

4a. Click **Add device** and proceed to step 7.

Find it via Broadcasting:

4b. 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**.

7. The **Add device wizard** is launched.
   Enter the **IP address** of the SafeCom Controller. Click **Next**.
8. Information is retrieved from the device to establish the type of device.
   Click **[change]** as the **SafeCom type** needs to be changed from **SafeCom Controller** to **SafeCom Go Sharp**.
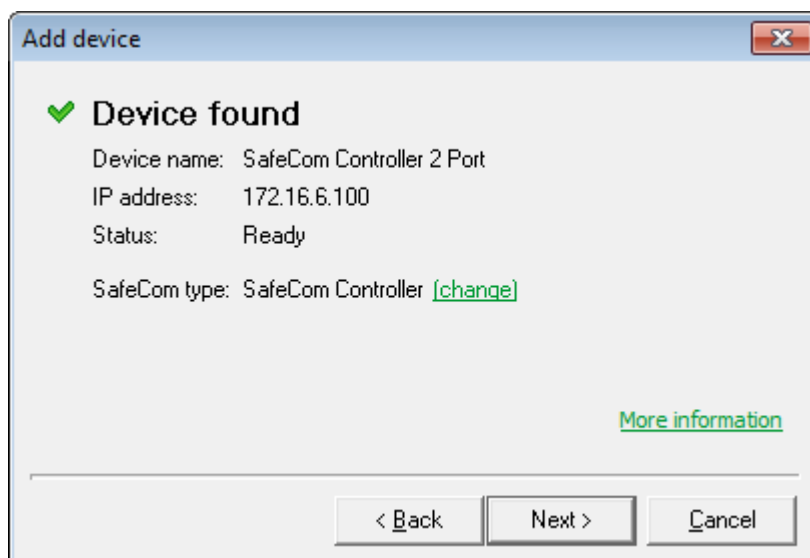
9. Select **SafeCom Go Sharp** as the type of SafeCom device. Click **Next**.

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

    Note The SafeCom Controller MUST reference the Sharp device by a fixed IP address or a fixed fully qualified hostname.
    Example: mysharp.safecom.eu.

11. Information is retrieved from the Sharp device. Click **Next**.
12. For the device enter the **User name** (default is admin) and **Password** (default is admin). On older devices the default password is Sharp.
13. On the **Settings** tab specify the properties of the device (**Duplex supported** and **Color supported**).
14. Click **Add** to register the device and save it in the database.

After approx. 1 minute the SafeCom Controller has restarted and you can verify the connection to the Sharp MFP by pressing the **test** button once on the SafeCom Controller's rear panel.

15. Configure the Sharp web interface.

Configure the Sharp device web interface

New Sharp devices

Follow the steps below to configure the web interface on new Sharp devices. If you have an old Sharp device, refer to 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. For the device enter the **User name** (default is admin) and **Password** (default is admin). 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].

---

[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.

6. Change **External Account Control** to **Enable**.
7. Check **Enable Authentication by External Server**.
8. In **Application Name** enter **SafeCom Go Sharp.**
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**.
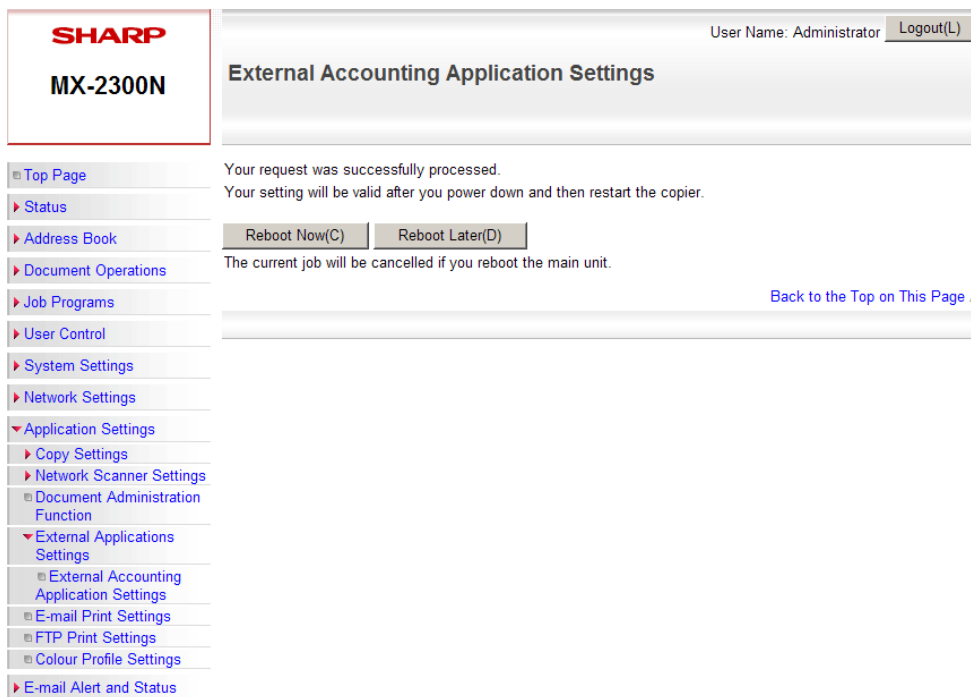
13. If **Standard Application Settings**[2] appears in the menu just above **External Accounting Application Settings** click **Reboot Later** and go to step 14.

    Otherwise click **Reboot Now** if you have completed the configuration and wait for the Sharp MFP to restart.

    Note 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.
14. Click **Standard Application Settings.**
15. 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 click **Pull Print** to see the configuration.

---

[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.

16. In Application Name enter Pull Print.

17. 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.

18. Leave **Timeout** on 20 seconds.
19. Click **Submit**.
20. Click **Reboot Now** and wait for the Sharp MFP to restart.

Note 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.

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, refer to Configure the Sharp device web interface.

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**. Enter the **User name** (default is admin) and **Password** (default is Sharp). On newer models the default password is admin. Click **OK.**
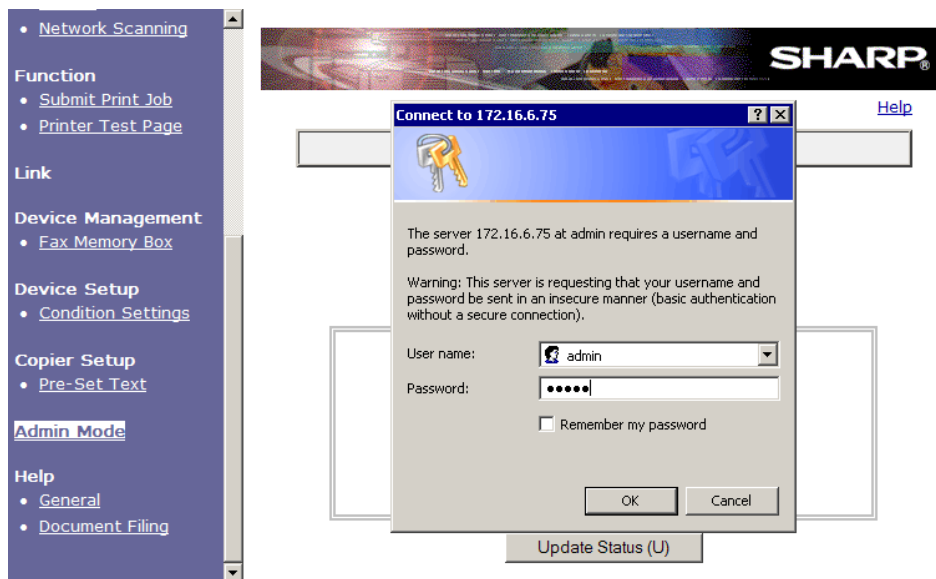
3. Scroll to and click **External Applications**.

4. Click **External Accounting³.**
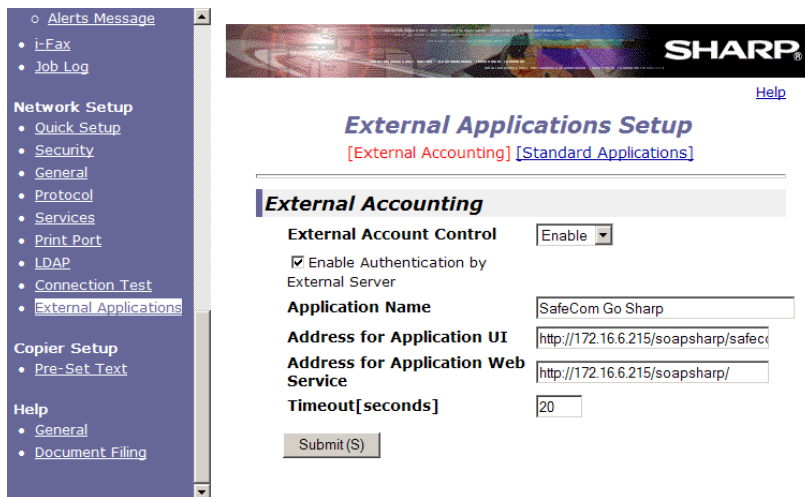
5. Change External Account Control to Enable.
6. Check Enable Authentication by External Server.
7. In Application Name enter SafeCom Go Sharp.
8. In Address for Application UI enter the reference to a specific file on the connected SafeCom Controller. The address is:

   ```
   http://<ip address>/soapsharp/safecom.scx
   ```

   where <ip address> should be replaced with the IP address of the SafeCom Controller.
9. 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.
10. Leave Timeout on 20 seconds.
11. Click Submit.

12. If Standard Applications⁴ appears as a link go to step 13. Otherwise power down and restart the Sharp MFP.

13. Click Standard Applications.
14. 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 check Pull Print and click Edit to see the configuration.

---

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.
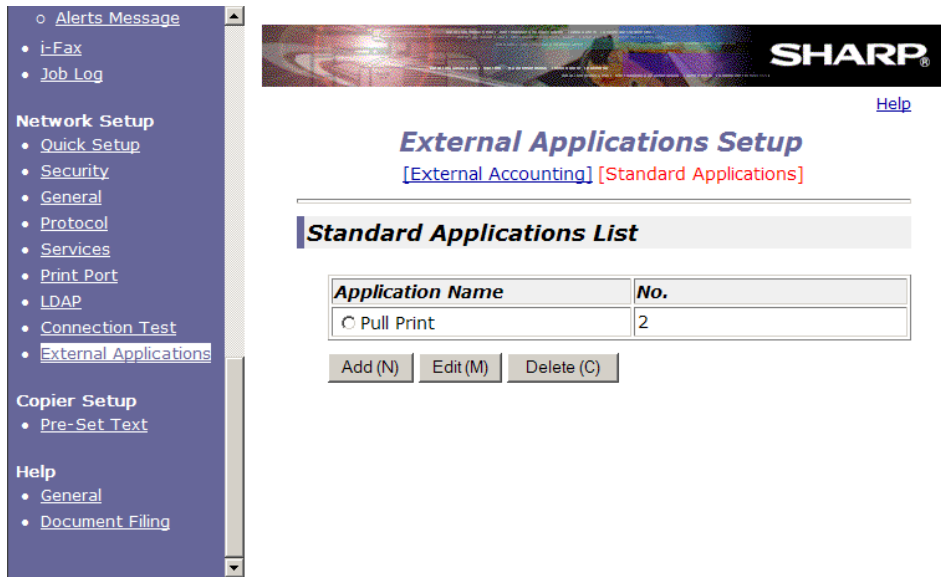
15. In **Application Name** enter **Pull Print**.
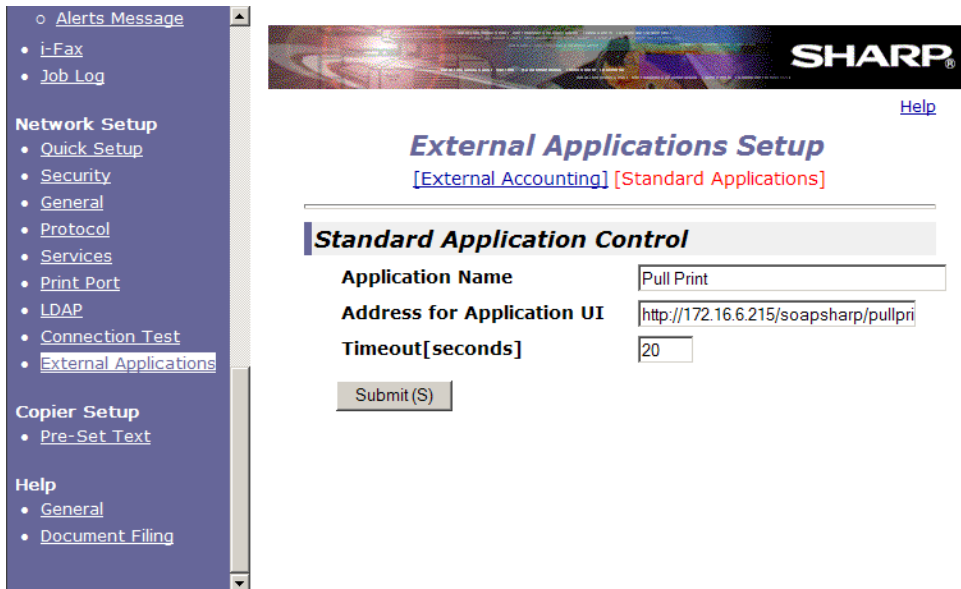
16. In **Address for Application UI** enter the reference to a specific file on the connected SafeCom Controller. The address is:

   ```
   http://<ip address>/soapsharp/pullprint.scx
   ```

   where <ip address> should be replaced with the IP address of the SafeCom Controller.

17. Leave **Timeout** on 20 seconds.
18. Click **Submit**.
19. 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. Use of JavaScript (Active Scripting) must be enabled.
2. Click **Advanced Configuration** to open the **Advanced Configuration** web page.

   Note 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**.

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

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 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** defaults to 60 seconds. Users will be logged out if they do not perform an operation on the Sharp MFP's touch-screen 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 via the network.

Printer IP Address must be that of the Sharp MFP.

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

Printer Manufacturer should be **SHARP.**

SafeCom Go must be **YES**.

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

Copy Idle Timeout is ignored.

High Speed Print Enabled 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.

Note 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.

Note 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**.

Note 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** (3.3.3) 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. Click **Save and Continue**.
3. Click **Printer** and check **Network – Port 9100**.
   Enter the **Printer IP address**.
4. Click **Save and Continue**.
5. Click **Restart**.

After approx. 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**.

Note 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 is maximum 8 characters.
4. Click **Save and Continue**.
5. Click **Restart**.

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

Assign a fixed IP address to the SafeCom Controller

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

1. Open the **Advanced Configuration** web page.
2. Click **TCP/IP**.
3. Check **Manual** and enter the **IP address** etc.
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 approx. 1 minute while SafeCom initializes. If the control panel on the Sharp MFP does not reflect the change in the login screen then refresh the screen by pressing the **JOB STATUS** button on the Sharp MFP and then 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** and change **Use auto** configuration to **YES**.
3. Click **Save and Continue**.
4. Click **Restart**.

Enable High Speed Print

1. Open the **Advanced Configuration** web page.
2. Click **Printer** and change **High Speed Print Enabled** should be **YES** if print data is to be sent directly (and unencrypted) to the device from the SafeCom server rather than through the SafeCom Controller.
3. Click **Save and Continue**.
4. Click **Restart**.

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

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 SafeCom Controller's test button 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.

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

Uninstall SafeCom Go Sharp

1. Open the Sharp MFP's web page and login.
2. Click **Application Settings**, and then **External Applications Settings**.
3. If there is no **Standard Application Settings**[5] menu item go to step 6.
4. Click **Standard Application Settings.**
5. Check **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.

   Note: 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.

Using SafeCom Go Sharp

Sharp device with SafeCom Device Server

Login

The different login sequences are described in the following. The Welcome screen is by default enabled, 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 touch-screen or keypad.
4. Tap **OK**.

Log in with ID code:

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

Log in with Windows:

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

Note Username and password cannot be blanks.

Main menu

Once logged in you can select an option from the touch-screen.
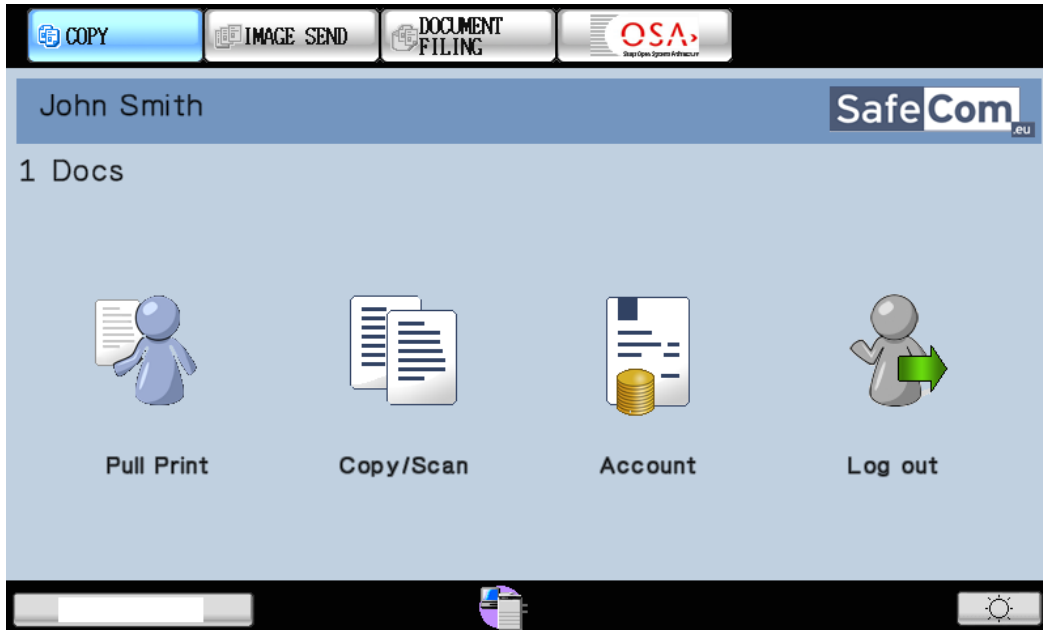
- Tap **Pull Print** to print individual documents.
- Tap **Copy / Scan …** to start copy or scan.
- Tap **Account** to select billing code.
- Tap **Log out** to log out.

Pull Print - Document list

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

1. Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list.
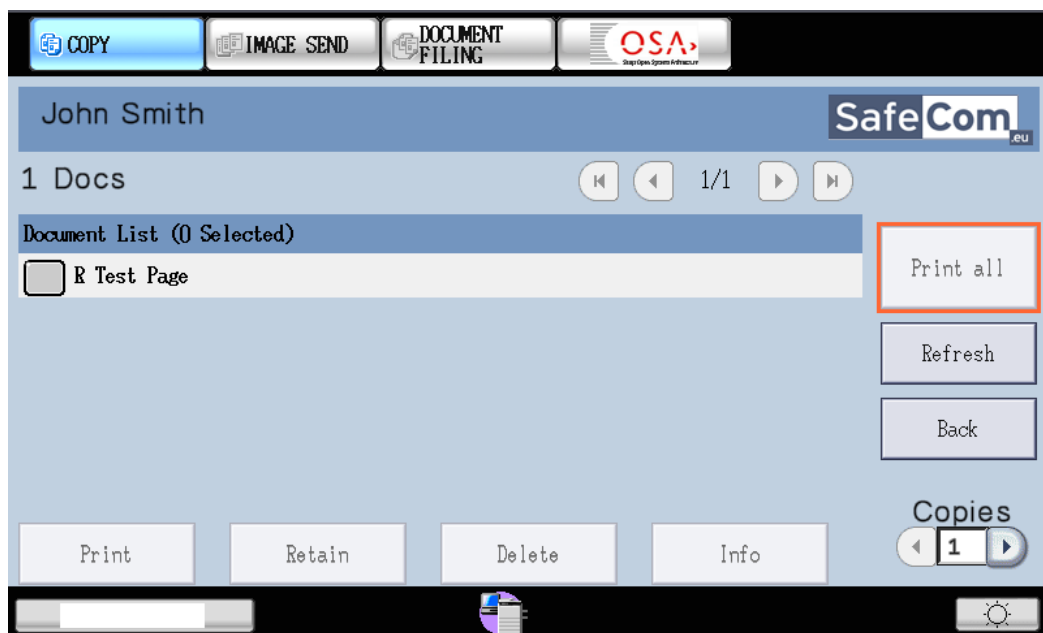
In the above example the preceding **R** shows the document is retained. A delegated document will have a preceding **D.** Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding **G**.

- 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.

Note
- 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 chooses to for example copy 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 choose from the list of the user's favorite billing codes. They are listed in alphabetical order.
3. Tap **Last used** to choose 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 choosing 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.

Note 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** checked on the **Settings** tab, and on the **Device properties** must have **Client Billing** checked on the **License** tab. 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 touch-screen. Tap **OK**.
3. Tap **OK**.

Enter PUK code and PIN code:

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **PIN code**.
4. Enter **PIN code** on the touch-screen. Tap **OK**.
5. 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 touch screen.
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 defaults to 30 seconds. The logout process is initiated if no buttons are tapped for this period.

To log out:

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

Sharp MX devices with MX-AMX2 license

Login

The different login sequences are described in the following. The Welcome screen is by default enabled (2.5), 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 touch-screen or keypad.
4. Tap **OK**.

Log in with ID code:

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

Log in with Windows:

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

Note
- Username and password fields cannot be left 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 touch-screen.

- 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.

1. 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 choose from the list of the user's favorite billing codes. They are listed in alphabetical order.
3. Tap **Last used** to choose 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 choosing 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.
4. Finish the job at the device.

Note 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** checked on the **Settings** tab, and on the **Device properties** must have **Client Billing** checked on the **License** tab. 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 touch-screen. Tap **OK**.
3. Tap **OK**.

Enter PUK code and PIN code:

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **PIN code**.
4. Enter **PIN code** on the touch-screen. Tap **OK**.
5. 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 touch screen.
4. Tap the **Password** field and enter the password.
5. Tap the **Domain** field and enter the domain.
6. Tap **OK**. To abort card registration tap **Cancel**.

Logout

There is a configurable **Timeout** that defaults to 30 seconds. The logout process is initiated if no buttons are tapped for this period.

To log out:

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

Sharp device with SafeCom Controller

Control panel
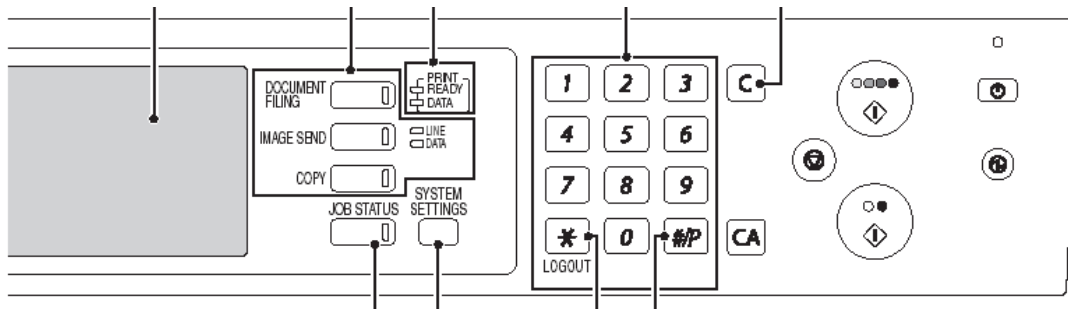
Login

The different login sequences are described in the following.

Log in with card:

1. Use card reader.

Log in with card and PIN code:

1. Use card reader.
2. Tap **PIN code**
3. Enter **PIN code** on the touch-screen. Tap **OK**.
4. Tap **OK**.

Log in with ID code:

1. Tap **ID code**.
2. Enter **ID code** on the touch-screen. Tap **OK**.
3. Tap **OK**.

Log in with ID code and PIN code:

1. Tap **ID code**.
2. Enter **ID code** on the touch-screen. Tap **OK**.
3. Tap **PIN code**
4. Enter **PIN code** on the touch-screen. Tap **OK**.
5. 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 touch-screen. Tap **OK**.
2. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.
3. Tap **OK**.

Note Username and Password fields cannot be left blank.

Main menu

Once logged in you can select an option from the touch-screen. Tap **Print All** to print all documents (except any retained documents). Documents are printed in chronological order (oldest first).
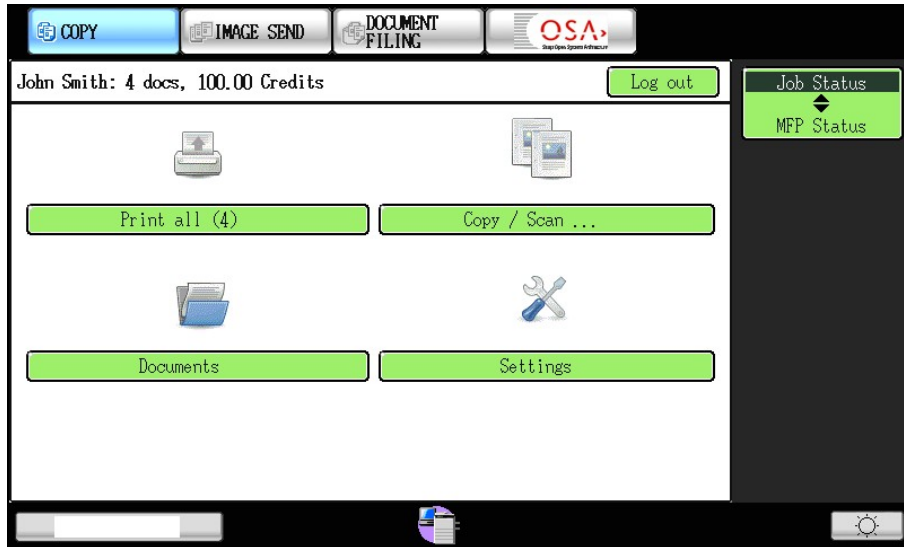
- Tap **Documents** to print individual documents.
- Tap **Copy / Scan …** to start copy or scan.
- Tap **Settings** to see settings.
- Tap **Log out** to log out.

Pull Print - Document list

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

1. Tap **Documents**.

Documents appear in chronological order with the newest at the top of the list.
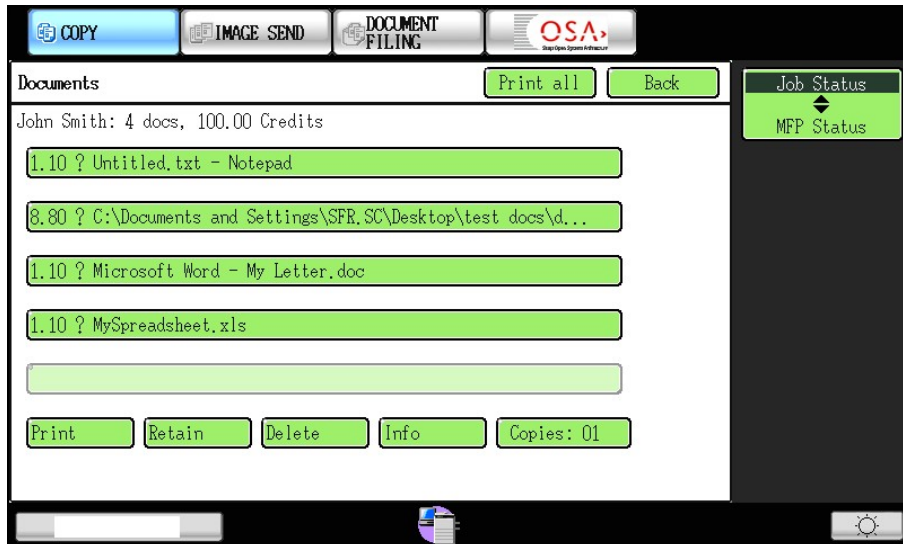
2. Tap **Print All** to print all documents, excluding any retained documents. Documents are printed in chronological order (newest first).
3. Tap **Print** to print the selected documents.
4. Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
5. Tap **Delete** to delete the selected documents.
6. Tap **Info** to see information about the selected documents, including cost, driver name, use of color and duplex.
7. Tap **Back** to return to the main screen.
8. Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.
9. In the document list a document with a preceding **R** shows the document is retained. The number is the cost of the document. A delegated print is marked with a preceding **D**. Tap the Info button to see information about who delegated the document. A group print document will have a preceding **G**.

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 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.

Note
- 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) will remove 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 chooses to for example copy 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.

Logout

There is a configurable **Timeout** that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To logout actively:

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

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 asked to enter his PUK code.

Enter PUK code:

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **OK**.

Enter PUK code and PIN code:

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **PIN code**.
4. Enter **PIN code** on the touch-screen. Tap **OK**.
5. Tap **OK**.

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

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

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

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

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

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

SafeCom Administrator: Unable to locate all SafeCom devices

1. In **SafeCom Administrator** click on the **Preferences** menu, **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. Obtain the SafeCom Controller's MAC address. It is printed on the white label on the bottom of the SafeCom Controller. The MAC address is a 12-digit hexadecimal number. Example: 00C076FF00F2. The network administrator can login to the DHCP server and see the IP address that is assigned to the SafeCom Controller.
Once you have the IP address click **Add device…** in **SafeCom Administrator**.

Copy jobs are not tracked

Please check the following:

- On the SafeCom Controller's **Printer** web page **Copy Enabled** is **YES**.
- In **SafeCom Administrator Tracking** is checked on the **License** tab in the **Device properties** dialog.
- In **SafeCom Administrator** cost control is set to **Tracking** or **Pay** on the **Settings** tab in the **User properties** dialog.

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, check the set up of **User properties** and **Device properties** in the **SafeCom Administrator**.

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

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 touch-screen on the Sharp MFP reports: "Could not access accounting server. Contact your administrator".

- Please verify that the SafeCom Controller is powered on, network connected and working.
- Please 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 property deviceserver.serverAddress in the config.ini file. This forces the Device Server to use the given IP when configuring devices. Refer to Device Server config.ini.

Device Server: Error when upgrading existing device server installation

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

"Error in action StopWindowsService"

The following must be completed before running the installer again:

1. Kill the installer process with the following command:

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

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

```
net stop scDeviceServer
```

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

```
net start scDeviceServer
```

4. Re-run the SafeCom Device Server installer.

Device Server: Pull Print icon is not available

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, you can also check the availability of the Account icon similarly. Ensure that the **BillingEnabled** property of the device is set to **True** via 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

Check and ensure that the **Auto Clear Setting** timer is lower than the **Auto Power Shut-Off** timer.

Regulatory information

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

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

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

CAUTION: Changes or modifications not expressly approved by SafeCom a/s could void the user's authority to operate this equipment according to part 15 of the FCC rules.
This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to take whatever measures may be required to correct the interference at his 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.