Kofax SafeCom Go Konica Minolta

Administrator’s Guide

Version: 9.12.0

Date: 2020-12-11

Table of Contents

Preface

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

Related documentation

The full documentation set for Kofax SafeCom Go Konica Minolta 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 Konica Minolta

- *Kofax SafeCom Go Konica Minolta User’s Guide*
  User’s guide on how to use SafeCom Go Konica Minolta.

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 Konica Minolta

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

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

Requirements

- SafeCom Go Konica Minolta supports OpenAPI 2.1 or higher MFPs.
- SafeCom device license.
- SafeCom ID device license.
- The MFP must be prepared so it allows use of OpenAPI, SSL on port number 50003 and print without authentication.
- The appropriate ID Device must be connected to the MFP’s USB port if users are to login by card.
- SafeCom G4 Server version S82 070.500*02 or later.
- SafeCom Device Server version S82 060.070*02 or later.
- The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.7 or later. If SafeCom Device Server is installed on a 64-bit operation system, you must install the 32-bit Java version included with the installer.

Supported ID devices

- **HID Reader (AU-201H):** To install and get the reader to work on a Konica Minolta device, a Loadable driver must be installed. This loadable driver is device dependent and also provided by Konica Minolta.
- **Other ID Devices:** Please contact Kofax Support.

The Konica Minolta device must be configured to use ID device.

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

Preparing the MFP

The MFP must be prepared as follows:

- Allow use of OpenAPI.
- Ensure that SSDP protocol is switched on.
- Use SSL on port number 50003 (assuming an SSL certificate is installed).
- Allow print without authentication.

Note

- The instructions below may vary between the different models. If in doubt, please consult the appropriate documentation from Konica Minolta.
- These steps are required on a fresh device or a device that has had its hard disk drive formatted. The settings are preserved when the printer firmware is updated.

OpenAPI settings

1. On the MFP’s touch screen open the **Administrator settings.**
2. Enter the administrator password.
3. Select **System connection**
4. Select **Open API settings**
5. Change the setting from **Restrict** to **Allow**.
6. Ensure that the **External Application Connection** is set to **Yes** (availability of this option depends on device model).

Ensuring SSDP is switched on

1. Open the web page of the MFP and log in as administrator.
2. Click the **Network** tab.
3. Select **SSDP settings**.
4. Ensure that **SSDP** is switched to **On**.

Enable SSL certificate:

1. Open the web page of the MFP and login as administrator.
2. Click the **Security** tab.
3. Click **PKI Settings**.
4. Click **Device Certificate Setting**.
5. Create **New Registration** of SSL certificate.
6. In **SSL Setting** choose **Admin mode and User mode.**
7. Click the **Network** tab.
8. Click **OpenAPI Settings**.
9. Set **SSL** to **SSL Only**.
10. Click **TCP Socket Setting**.
11. Check **Use SSL/TLS**.

Note For Bizhub model C224, you need to remove the default/original SSL certificate after creating and enabling the new one.

On Konica xx50 devices, do the following:

1. Open the web page of the MFP and login as administrator.
2. Click the **Security** tab.
3. Create a new SSL certificate, using a similar method as outlined above.
4. Click the **Network** tab.
5. Ensure that **SSDP** is enabled.

6. Browse to the HTTP settings and activate SSL.
7. Click **OpenAPI Settings**.
8. Set **SSL** to **SSL Only**.
9. Click **TCP Socket Setting**.
10. Check **Use SSL/TLS**.
11. Open the SafeCom Device Server web page, and add the device to SafeCom.
12. Click **Save**.

Allow print without authentication:

1. On the MFP's touch screen press the **Utility/Counter** button.
2. Tap **Administrator Settings**.
3. Enter the **Administrator Password** and tap **OK**.
4. Tap **User Authentication / Account Track**.
5. Set **Print without Authentication** to **Allow**.
6. Tap **OK** and restart the MFP.

On bizhub C35: Configure driver

Note Do not configure the driver until you have added the C35 to the device server, see Add device to the SafeCom Device Server.

1. In **Windows** open **Devices and Printers** then right-click the C35 device and select **Printer properties**.
2. In the **KONICA MINOLTA bizhub C35 Properties** window, go to the **Configure** tab.
3. In the **Device Option** section select **User Authentication**, then in the **Setting** drop-down list select **On (Enhanced Server)**.
4. Click the **Acquire Settings** button.
5. In the **Acquire Settings** window select **Specify IP Address or Printer Name** and then type in the bizhub C35's IP address manually. Click **OK.**
6. In the **KONICA MINOLTA bizhub C35 Properties** window click **Apply**, then go to the **General** tab and click the **Preferences…** button.
7. In the **KONICA MINOLTA bizhub C35 Printing Preferences** window go to the **Basic** tab and click **Authentication/Account Track**.
8. In the **Enhanced Authentication Server Settings** window remove the checkmark from **Public User.**
9. In **User Code** type in anything. Do *not* click **Verify** as it will not work. Click **OK**.
10. In the **KONICA MINOLTA bizhub C35 Printing Preferences** window click **Apply** and then **OK.**
11. In the **KONICA MINOLTA bizhub C35 Properties** window click **OK.**

Note Changing the port configuration after having configured the driver may result in the device losing the authentication configuration, which can be restored by repeating the steps above.

On bizhub C284e and C654e: Configure driver

Note Do not configure the driver until you have added the C284e/C654e to the device server, see Add device to the SafeCom Device Server.

1. In **Windows** open **Devices and Printers** then right-click KM device and select **Printer properties**.
2. In the KONICA MINOLTA <devicemodel> Properties window, go to the Configure tab.
3. In the **Device Option** section select **Model**, then use the **Setting** dropdown list to select the device model.
4. Select **User Authentication**, then in the **Setting** drop-down list select **On (Enhanced Server)**.

5. Click the **Obtain Settings** button.
6. In the **Obtain Settings** window uncheck the **Auto** checkbox, select **Specify IP Address or Printer Name** and then type in the device IP address manually. Click **OK**.
7. In the **KONICA MINOLTA <devicemodel> Properties** window click **Apply**, then go to the **General** tab and click the **Printing Preferences…** button.
8. In the **Printing Preferences** window go to the **Basic** tab and click **Authentication/Account Track**.
9. In the **Enhanced Authentication Server Settings** window remove the checkmark from **Public User.**
10. In **User Code** type in anything. Do not click **Verify** as it will not work. Click **OK**.
11. In the **Printing Preferences** window click **Apply** and then **OK**.
12. In the **Properties** window click **OK**.

Note Changing the port configuration after having configured the driver may result in the device losing the authentication configuration, which can be restored by repeating the steps above.

SafeCom Go Konica Minolta

Overview

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

Note The MFP must be prepared so it allows use of OpenAPI, SSL on port number 50003, and print without authentication (Refer to Preparing the MFP).

SafeCom Device Server installation

Install SafeCom Device Server:

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

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

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

   The default installation folder is:

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

   On **Windows 64-bit**:

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

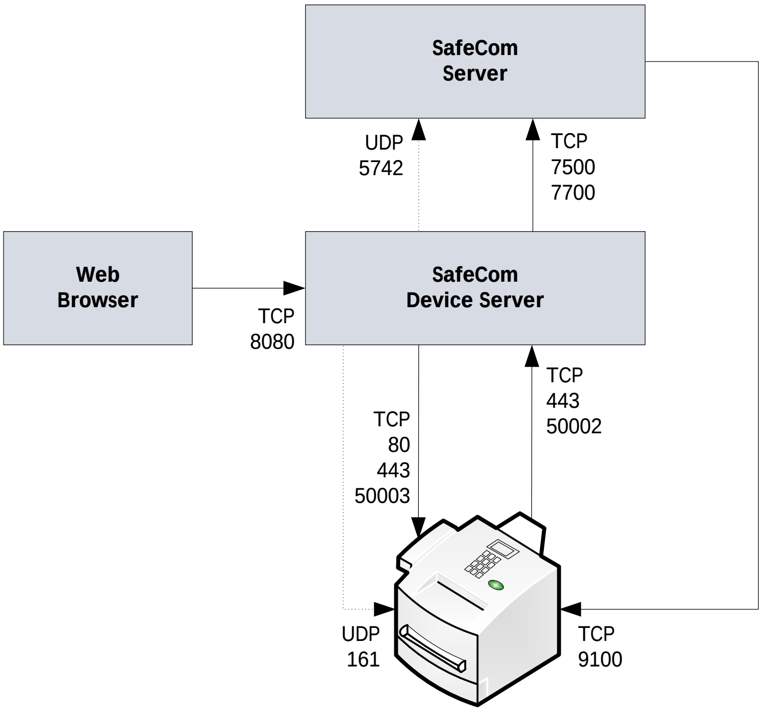
3. Click **Next**.
4. Choose destination folder. Click **Next**.
5. Detecting Java version. Click **Next**.
6. Review settings before copying of files starts. Click **Next**.
7. Click **Finish**.

Windows firewall - Ports that must be opened

If Windows Firewall is enabled it may prevent the **SafeCom 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. The command file must be **Run as administrator**. In the file you can see which TCP and UDP ports are opened.

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



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

Configure SafeCom Device Server

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

Log in to SafeCom Device Server

To log in to SafeCom Device Server:

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

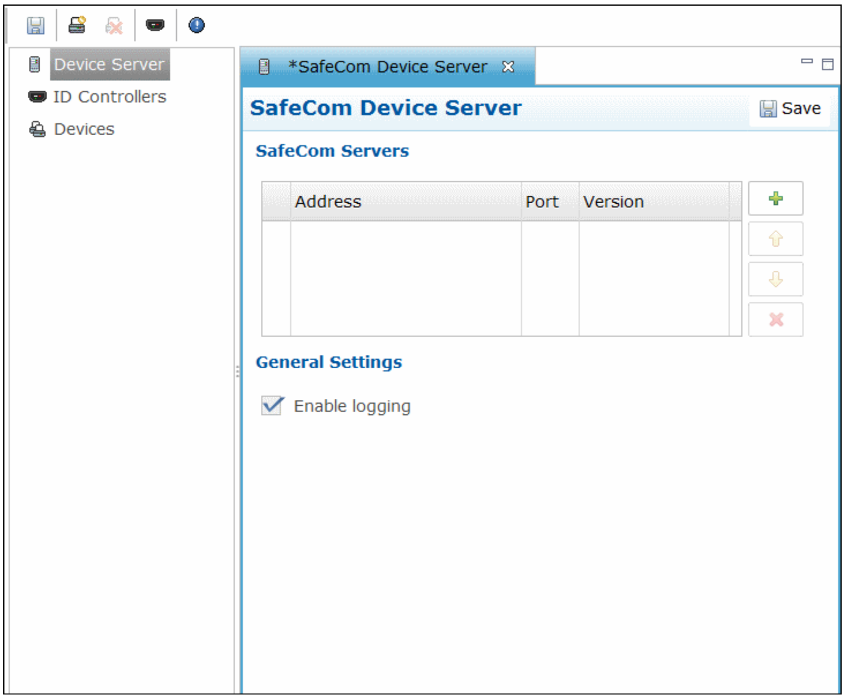
   Example: `http://localhost:8080/safecom`

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

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

Add SafeCom Server

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



☑ Enable logging

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 “Grouping device servers” in the *SafeCom G4 Administrator’s Guide*.

The SafeCom Server is now added, and the next step is to add a device to the device server (see Add device to the SafeCom Device Server).

Device Server config.ini

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

After editing the config.ini file, the SafeCom Device Server service must be restarted 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 the SafeCom Device Server

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

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

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

Device icons

In the **SafeCom Device Server** the following device icons represents the status of the device.

👤 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 the SafeCom Administrator

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

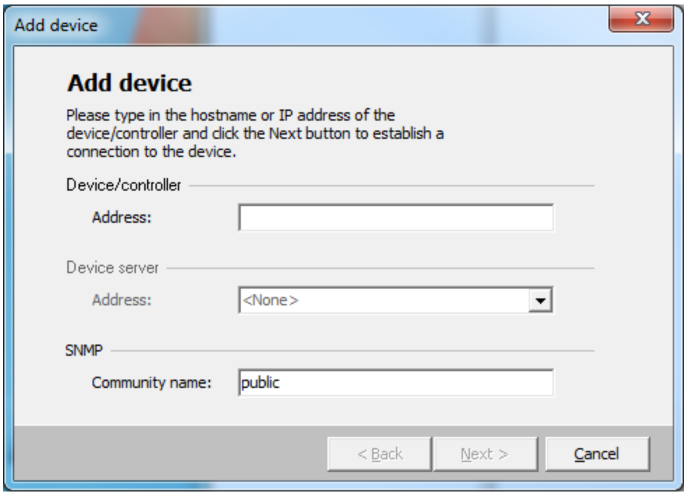
If the device server is not yet added in the SafeCom Administrator, see the instructions above for configuring a SafeCom Device Server and adding it to a SafeCom Server. If the device server is already added in the SafeCom Administrator, go to **Add device server device** below.

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**.



Add device

Please type in the hostname or IP address of the device/controller and click the Next button to establish a connection to the device.

Device/controller

Address:

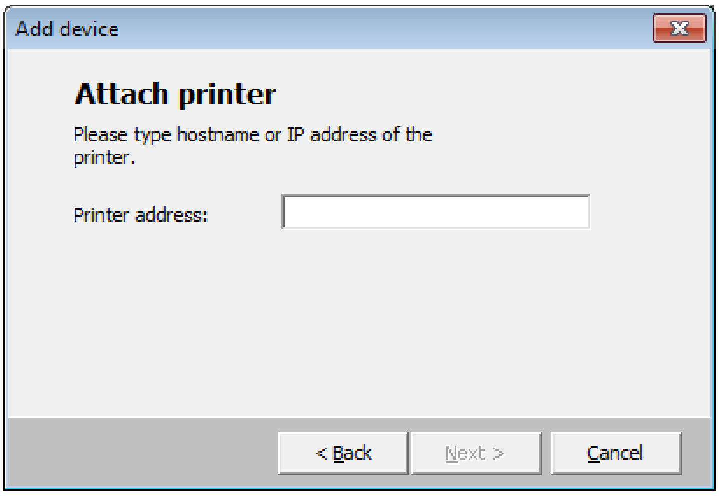
Device server

Address: <None>

SNMP

Community name: public

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**.

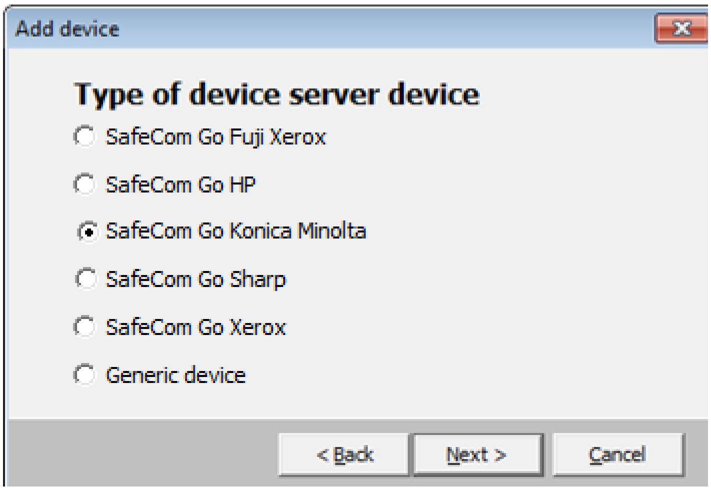


Attach printer

Please type hostname or IP address of the printer.

Printer address:

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



Type of device server device

○ SafeCom Go Fuji Xerox

○ SafeCom Go HP

● SafeCom Go Konica Minolta

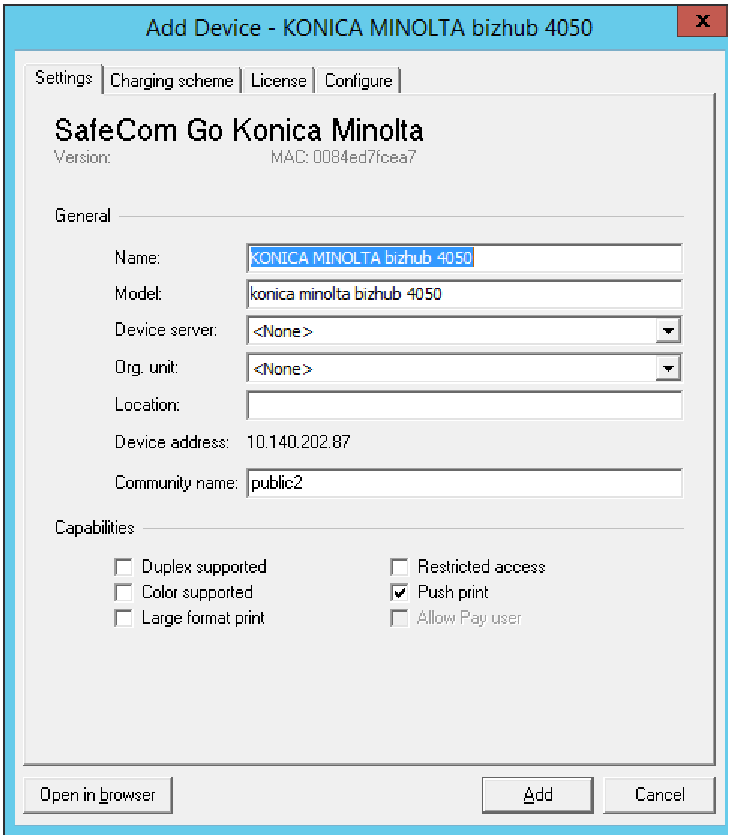
○ SafeCom Go Sharp

○ SafeCom Go Xerox

○ Generic device

7. Enter the username and password, as specified on the device web page and click **Next**.

8. The device properties dialog now opens. Make sure to specify on the **Settings** tab the device server and the capabilities of the device.



SafeCom Go Konica Minolta

Version:

MAC: 0084ed7fcea7

General

Name: KONICA MINOLTA bizhub 4050

Model: konica minolta bizhub 4050

Device server: <None>

Org. unit: <None>

Location:

Device address: 10.140.202.87

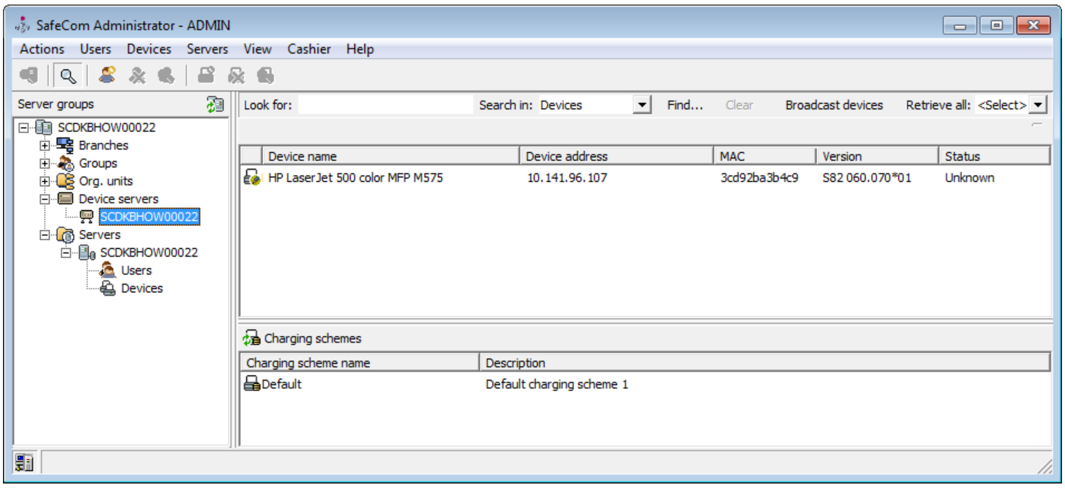
Community name: public2

Capabilities

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

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.



Look for:

Search in: Devices

Retrieve all: <Select>

Device name	Device address	MAC	Version	Status
HP LaserJet 500 color MFP M575	10.141.96.107	3cd92ba3b4c9	S82 060.070*01	Unknown

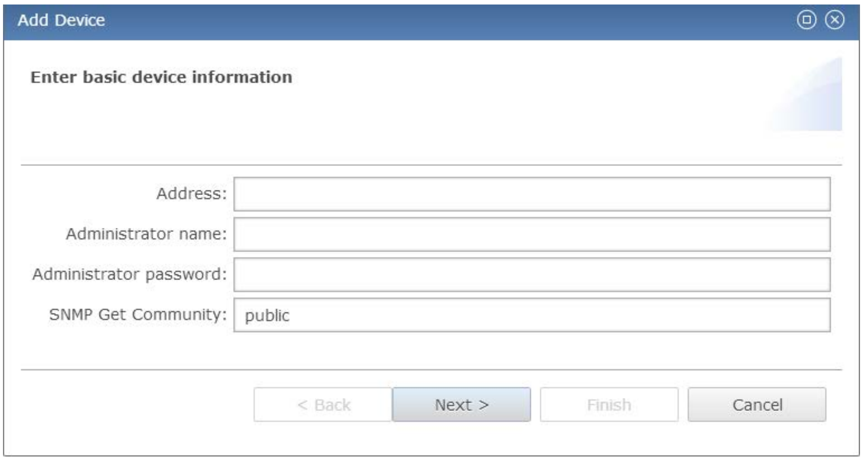
Charging schemes

Charging scheme name	Description
Default	Default charging scheme 1

10. Go to Configure device in SafeCom Device Server to continue with the configuration of the device.

Add device via the SafeCom Device Server

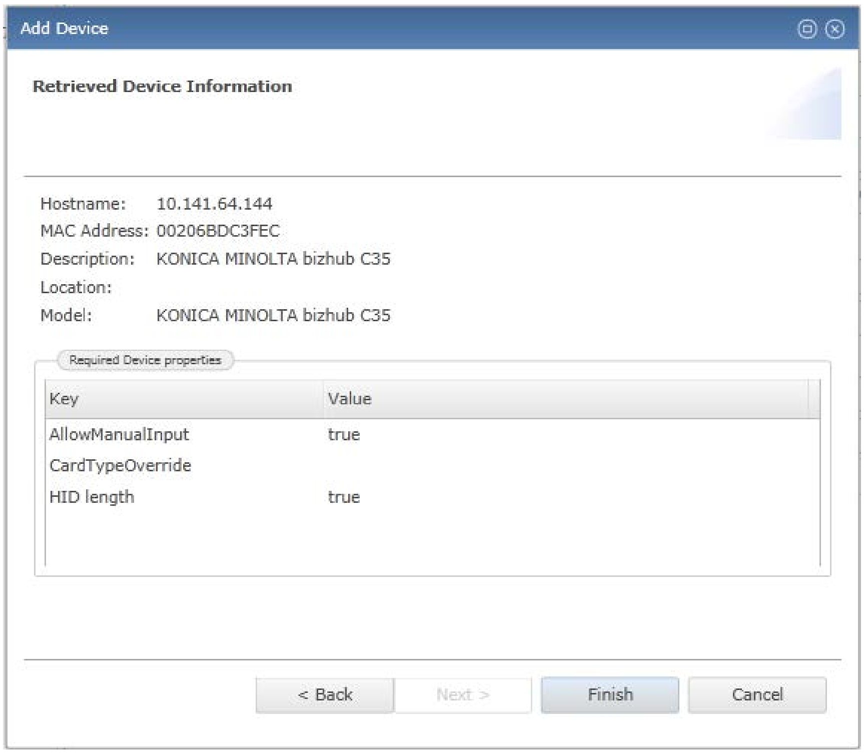
1. Click **Device Server** in the left menu.
2. Click the **Add device** button and the **Add device wizard** launches.
3. Enter the hostname or the IP address of the device. If you want to use dynamic IP address, then enter the device hostname in the **Address** field.
4. Enter the administrator name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



Enter basic device information

Address:	
Administrator name:	
Administrator password:	
SNMP Get Community:	public

6. Information is retrieved from the device to establish the type of device. Make the necessary adjustments to the **Required Device properties** (2.5).



Retrieved Device Information

Hostname:	10.141.64.144
MAC Address:	00206BDC3FEC
Description:	KONICA MINOLTA bizhub C35
Location:	
Model:	KONICA MINOLTA bizhub C35

Required Device properties

Key	Value
AllowManualInput	true
CardTypeOverride	
HID length	true

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

Note 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.

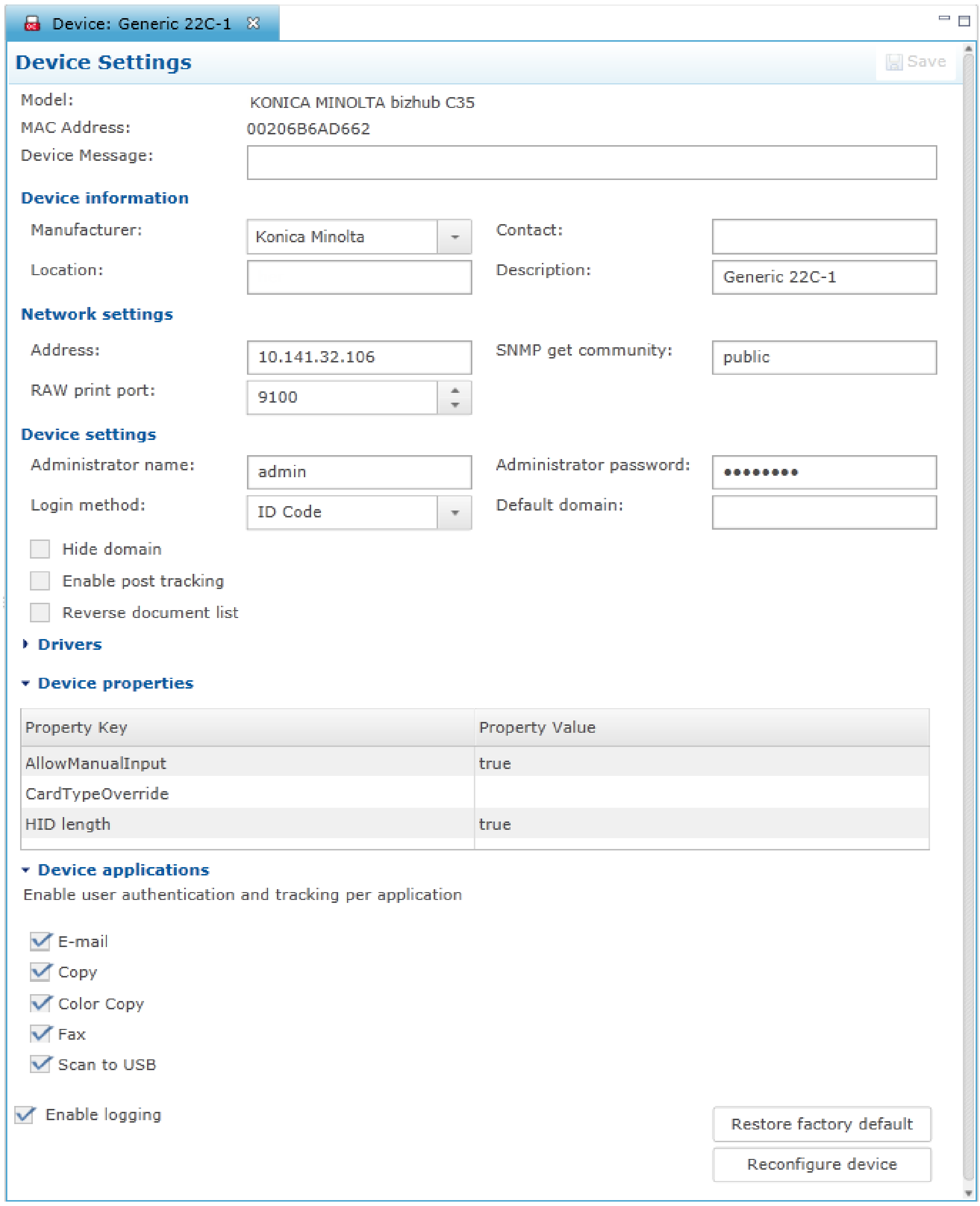
Configure device in SafeCom Device Server

The **Device** tab is used to configure SafeCom Go Konica Minolta 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 At the device: printing fails mid-job for a resolution.

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

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**.



Device Settings

Model: KONICA MINOLTA bizhub C35

MAC Address: 00206B6AD662

Device Message:

Device information

Manufacturer: Konica Minolta

Contact:

Location:

Description: Generic 22C-1

Network settings

Address: 10.141.32.106

SNMP get community: public

RAW print port: 9100

Device settings

Administrator name: admin

Administrator password: ••••••••

Login method: ID Code

Default domain:

□ Hide domain

□ Enable post tracking

□ Reverse document list

▸ Drivers

▾ Device properties

Property Key	Property Value
AllowManualInput	true
CardTypeOverride	
HID length	true

▾ Device applications

Enable user authentication and tracking per application

☑ E-mail

☑ Copy

☑ Color Copy

☑ Fax

☑ Scan to USB

☑ Enable logging

Change the settings according to the following descriptions:

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

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

- **Device settings**
  - **Administrator name:** The user name with which the administrator can log in to device.
  - **Administrator password (mandatory):** The device password with which the administrator can log in to device.
  - **Login method:** This determines how users log in. Choose between:
    - **Card**
    - **ID code**
    - **Card or ID code**
    - **Card or Windows:** Allows the user to log in by either card or by entering their Windows username, password, and domain.

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

  - **Default domain:** Specify the domain to pre-fill the domain for users when logging into a device.
  - **Language:** Specify a specific language if you want SafeCom Device Server to override the language on the device.
  - **Hide domain:** Usable if you specified a default domain. Check to allow the users to log in without typing in the domain.
  - **Enable post tracking:** This is relevant only with SafeCom Tracking. Refer to the *SafeCom G4 Administrator’s Manual.*
  - **Reverse document list:** Check to show the first printed documents at the top of the document list.

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

- **Device Properties:**
  - **AllowManualInput:** Check to allow users to manually enter e-mail addresses and fax numbers.
  - **CardTypeOverride:** If using a card reader that is not supported by SafeCom, the administrator needs to specify which card type is used, since this cannot be identified automatically.

Property value	**Description**
FELICA_IDM	Felica
TYPE_A	MiFare

HID_PROX	HID
MAGNETIC_CARD	Magnetic

- **HID length:** If using a card reader that is not supported by SafeCom and HID cards, the administrator must specify the HID length, since this cannot be identified automatically

- **Device applications:** Lists the applications that users are allowed to access. Clear the applications that do not require user authentication.

  The settings under **Device applications** are tied to the welcome screen. If none of the check boxes are selected the welcome screen only shows the option to **Login** and, if enabled, **Windows login**.

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

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

  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:** Set all settings to their default value. Except from the password.

- **Reconfigure device:** Reference the device to the current SafeCom Device Server.

SafeCom Go Konica Minolta - How to

Register device

To register the device with the SafeCom solution, add the device in the SafeCom Administrator using **Add device**.

Change login method

The following section shows how to change the login method. If for example the device has a card reader installed, you must change the **Login method** to a method that includes **Card**.

Note This can only be done through the **SafeCom Device Server** web page and not through the **SafeCom Administrator**.

To change the login method:

1. Log in to **SafeCom Device Server**.
2. In the left pane, expand **Device Server** and click on the device to open the **Device** tab.
3. Change the login method as needed.
4. Click **Save**.

Note 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.**

Post tracking setup

For post tracking to work the printer driver MUST have **User Authentication** enabled and configured with a user named **safecompullprint**.

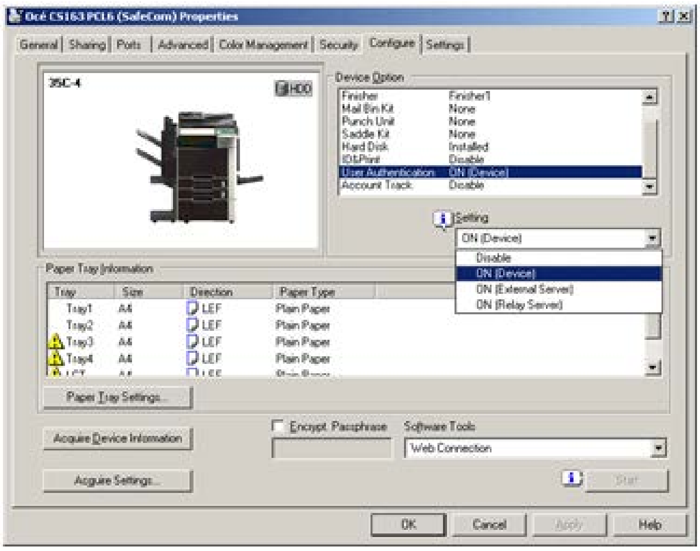
Note Be aware that in case of print jobs with mixed paper sizes, the device may not provide fully accurate post tracking information due to firmware limitations.

Enable Post tracking for the device:

1. Log in to **SafeCom Device Server**.
2. In the left pane expand **Device Server** and click on the device to open **Device** tab.
3. Check **Post tracking** and click **Save**.

Set up the printer driver:

1. Open the **Properties** dialog for the printer and click the **Configure** tab.
2. In the **Device Option** list scroll to and click **User Authentication**.
3. Change **Setting** to **ON (Device)** and click **Apply**.



Device Option

Finisher	Finisher1
Mail Bin Kit	None
Punch Unit	None
Saddle Kit	None
Hard Disk	Installed
ID&Print	Disable
User Authentication	ON (Device)
Account Track	Disable

Setting: ON (Device)

- Disable
- ON (Device)
- ON (External Server)
- ON (Relay Server)

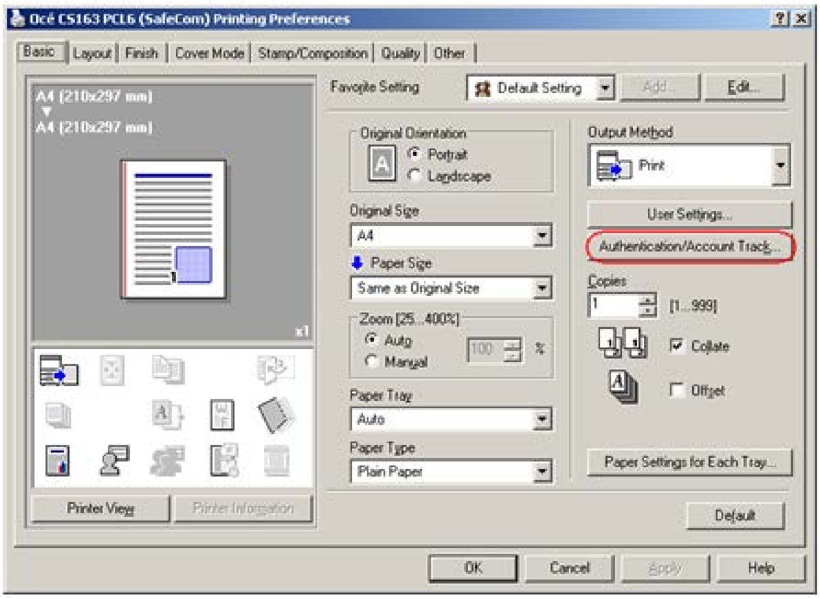
Paper Tray Information

Tray	Size	Direction	Paper Type
Tray1	A4	LEF	Plain Paper
Tray2	A4	LEF	Plain Paper
Tray3	A4	LEF	Plain Paper
Tray4	A4	LEF	Plain Paper

□ Encrypt Passphrase

Software Tools: Web Connection

4. Click on the **General** tab and select **Printing Preferences.**
5. On the **Basic** tab click **Authentication/Account Track.**



Favorite Setting: Default Setting

Original Orientation: ● Portrait ○ Landscape

Original Size: A4

Paper Size: Same as Original Size

Zoom [25...400%]: ● Auto ○ Manual 100 %

Paper Tray: Auto

Paper Type: Plain Paper

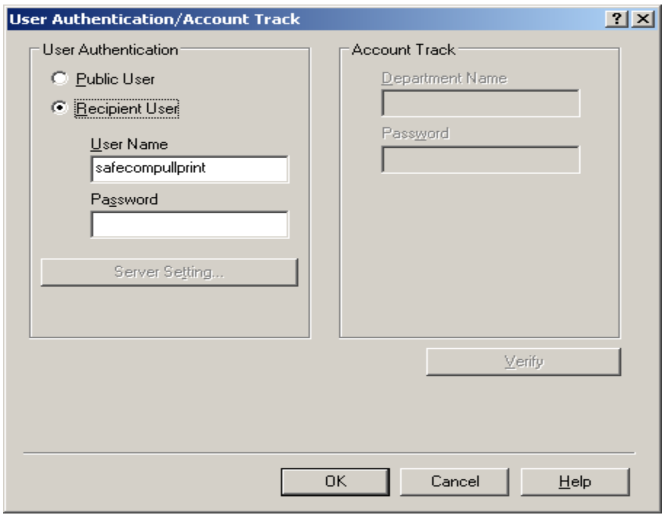
Output Method: Print

Copies: 1 [1...999]

☑ Collate

□ Offset

6. Select **Recipient User** and enter username as **safecompullprint** and click **OK**.



User Authentication

○ Public User

● Recipient User

User Name: safecompullprint

Password:

Account Track

Department Name:

Password:

Check device properties

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

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

Note Open in browser opens the web page of the device in a web browser. **Update software** is not relevant and should not be used. To update the **SafeCom Device Server** just install it again (see SafeCom Device Server installation).

Install card reader

This section is only relevant if users will login by card. Connect the ID Device directly to the external USB port located at the rear next to the network port. It may be necessary to remove the right-rear cover to access the USB port.

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.

1. On the MFP press the **Utility/Counter** button.
2. Tap **Meter Count**.
3. Tap **Check Details**.
4. Press the **Stop** button.
5. On the keypad enter 00 (zero zero).
6. Press the **Stop** button.
7. On the keypad enter 01 (zero one).
8. Press the **Stop** button.
9. On the keypad enter 9 (nine).
10. Tap **Management Function Choice**.
11. Tap **Authentication Device2**.
12. Tap **Card**.
13. Tap **END**.
14. Tap **Exit** on the Service Mode screen.
15. Power the device off.
    Wait 10 seconds or more before turning power on again.

Note Performing the above steps may change the **ID & Print** setting away from **OFF**. Please set it back to OFF (see below).

Set ID & Print to OFF

1. On the MFP press the **Utility/Counter** button.
2. Tap Administrator Settings.
3. Enter Password. Tap OK.
4. Tap User Authentication / Account Track.
5. Tap User Authentication Settings.
6. Tap Administrative Settings.
7. Tap ID & Print Settings.

8. Set ID & Print to OFF.
9. Tap **OK**.
10. Press the **Utility/Counter** button.

Open up for copy without authentication

There are two ways of opening up for copy without authentication on Konica Minolta:

Via General settings:

1. Press the **Function counter** button and then **Administrator settings**.
2. Enter the code '12345678'.
3. Select **User Authentication/Account track**.
4. Select **General settings**.
5. Tap **Public user Access** and then set it to **ON (without login)**.

Via User registration:

1. Press the **Function counter** button and then **Administrator settings**.
2. Enter the code '12345678'.
2. Select **User Authentication/Account track**.
3. Select **User Authentication Settings** and then **User Registration**.
5. Tap **000/Public** and then **Edit**.
6. Unselect **Print**.

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 Administator’s Manual*. You can control access rights to the following features:

- Copy
- E-mail
- Scan
- Fax

Note If **Scan** is enabled, **E-mail** will also become enabled, and the other way around. Controlling these two settings separately is not possible.

Uninstall SafeCom Go Konica Minolta

To uninstall the SafeCom Go Minolta software from the device:

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

SafeCom Go Konica Minolta device trace facility

Note Use the SafeCom trace facility only if SafeCom Support instructs you to do so.

Used for troubleshooting, the SafeCom trace facility is enabled through the **Configuration** web page:

1. Open the device web page and log in.
2. Click the **General** tab, and then click **SafeCom** in the menu to the left.
3. If the log is disabled, click the **Enable** button to the right.
4. To save the log, click **Show complete log**, select the log information and copy it into a *.txt file and save it.

Alternatively, 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
   ```

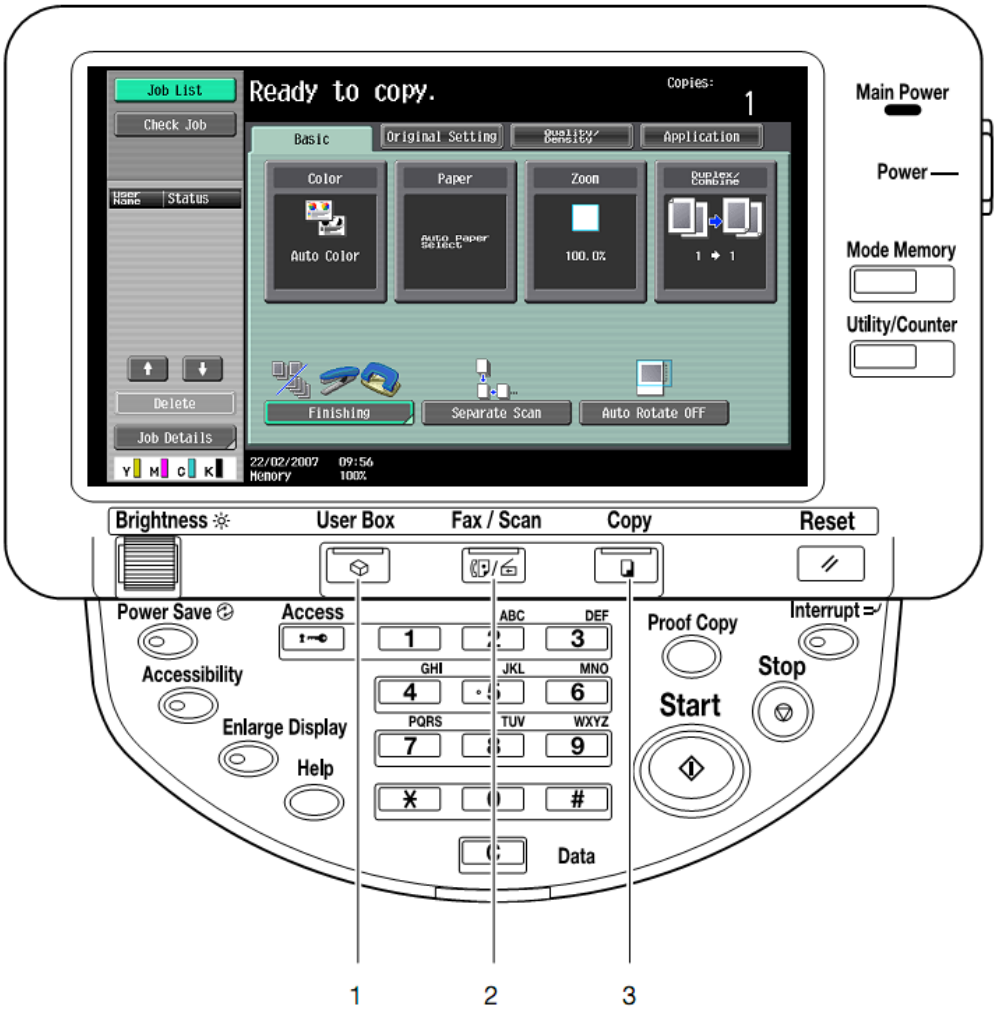
2. Double-click the `config.ini` file. In the open file, scroll to the bottom and add:

   - `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.

Using SafeCom Go Konica Minolta

Control panel



Login

Log in with card:

1. Use card reader.

Log in with card and PIN code:

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

Log in with ID code:

1. Tap **ID code** on the touch-screen.
2. Enter **ID code** on the screen and tap **OK**.
3. Tap **Login** or press the **Access** button 🔑

Log in with ID code and PIN code:

1. Tap **ID code** on the touch-screen.
2. Enter **ID code** and tap **OK**.
3. Tap **Login** or press the **Access** button 🔑
4. Tap **PIN code** on the touch-screen.
5. Enter **PIN code** and tap **OK**.

Log in with Windows:

If **Login method** is **Card or Windows** it is possible to login by either using your card or entering your Windows login credentials:

1. Tap **Username** on the touch-screen.
2. Enter **Username** and tap **OK**.
3. Tap **Password** on the touch-screen.
4. Enter **Password** and tap **OK**.
5. Tap **Domain** on the touch-screen.
6. Enter **Domain** and tap **OK**.

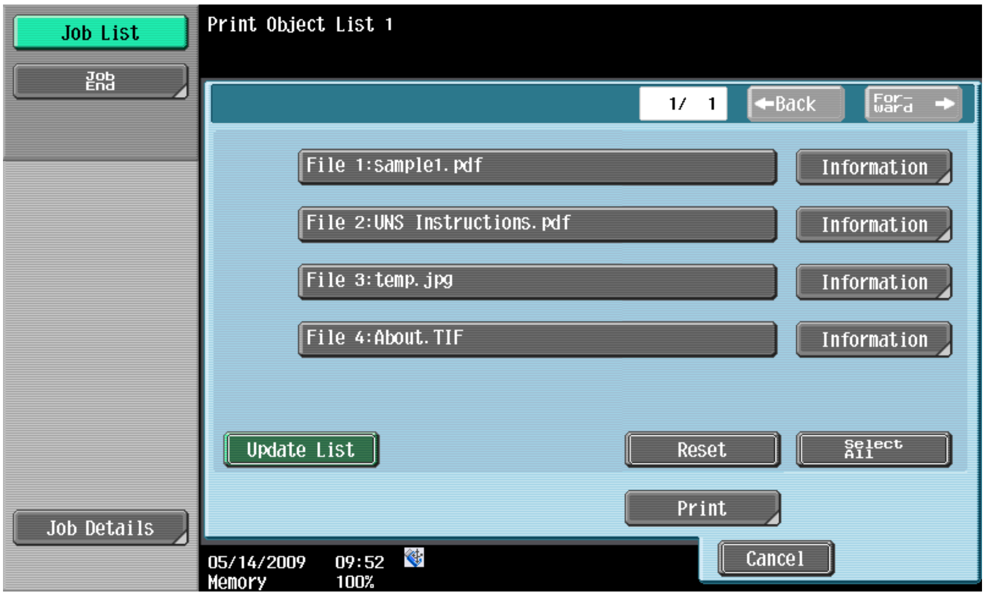
   Note Username and Password cannot be blanks.

Pull Print - Document list

Tap **Pull Print** to access the **Document list** that allows you to print individual documents. Documents appear in chronological order with the newest at the top of the list.

Note If there are more than 100 documents in the list of pull print documents, only the 100 most recent documents can be shown in the list. The **Print all** command still print all documents, and the document count is still the full amount of documents.

1. Tap **Select All** or select document(s). If there are more than 5 documents tap **Forward** to see additional documents.
2. Press the **Start** button to print the selected documents.
3. Tap **Job End** or press the yellow [//] **Reset** button to exit the document list.



Note The document list does look slightly different from the above.

In the in the document list a document with a preceding **R** shows the document is retained. A delegated document will have a preceding **D**. Tap the Info button to see information about who delegated the document. A group print document will have a preceding **G**.

- Tap **Reset** to deselect documents.
- Tap **Update List** to update the list of documents with pending documents that has finished spooling after the user logged in.
- Tap **Copies** to request multiple copies of the selected documents.
  To set the number of copies tap **Copies** and then press the **C** button to set copies to **0** and then enter the number of desired copies. Tap **OK** or **Cancel**.
- Tap **Delete** to delete the selected documents.
  To confirm that the documents should be deleted tap **Delete** or tap **Save** to cancel the operation.
- Tap **More**… and then **Info** to see information about the selected document, including cost, driver name, use of color and duplex. Tap **OK**. Tap **OK**.
- Tap **More…** and then **Retained** if you want document to remain on the list (server) after they have been printed. Tap **OK** and then **Update List.** A retained document is listed with a preceding **R**.

Copy

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

E-mail

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

Note E-mail is tracked and charged as if it was a Scan to folder job.

Logout

There is a configurable **Timeout** that defaults to 60 seconds and is controlled by the device. The logout process is initiated if no buttons are taped for this period. To logout actively:

- Press the **Access** button 🔑

Register card with PUK code

Register card with PUK code:

1. Use card reader. If the card is unknown and there is an available PUK code in the SafeCom system the user is asked to enter his PUK code.
2. Tap **PUK code** on the touch screen.
3. Enter **PUK code** and tap **OK**.
4. Tap **PIN code** on the touch screen.
5. Enter **PIN code** and tap **OK**.
6. The card is registered and you are asked to log in again.

Troubleshooting

This chapter contains troubleshooting hints for the SafeCom Go Konica Minolta product. Additional troubleshooting hints are available in the Troubleshooting chapter in the *SafeCom G4 Administrator’s Guide.*

SafeCom Help Desk Assistant

We want your SafeCom solution to be one that reduces not only print costs, but is also easy to support. In the following section, you will find useful troubleshoot hints.

Servlets

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

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

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

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

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

SafeCom Device Server does not start

Ensure that your Java Runtime Environment is working properly.

Authentication Version 2.0 Not Found

If you see this error message “Authentication version 2.0 not found” after updating F/W in the device, you need to change the Software Switch Setting to the following in the Service Mode on the device:

- Switch No.: 25
- HEX Assignment: 20

Change Software Switch Settings:

1. On the device press the **Function Counter** button.
2. Tap the **Meter Count** button on the display, and then **Check details**.
3. Enter the Service mode, by pressing the **Stop** button, enter '00', press **Stop** again, and then '01'.
4. In the service mode tap **System 2**.
5. Tap **Software Switch Settings**.
6. Type '25' in **Switch No.** field.
7. Type '20' in **Hex Assignment** field.
8. Tap **Fix**.

At the device: printing fails mid-job

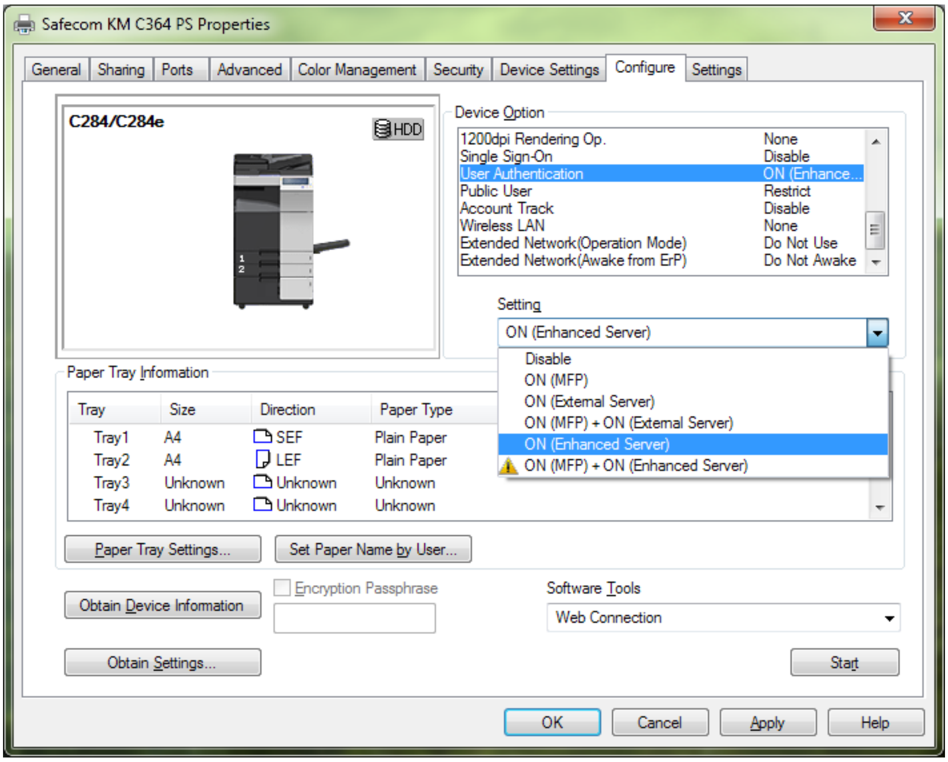
The Device Server periodically sends SNMP requests to devices in order to get information about their current state. Under certain circumstances, certain devices stop responding to these requests, resulting in a cancelled communication as well as failed print jobs. To solve this, add the following line to the `config.ini` file (located in `equinox` subfolder of the SafeCom installation folder):

```
deviceserver.printerStateCheckUnderPrinting=false
```

At the device: printing fails when post tracking is enabled

If you have post tracking enabled, and your print jobs fail, you may to reconfigure your device properties due to device-specific **User Authentication** naming.

1. Log in to **SafeCom Device Server**.
2. In the left pane expand **Device Server** and click on the device to open **Device** tab.
3. Ensure that **Post tracking** is checked and click **Save** (if applicable).
4. Open the **Properties** dialog for the printer and click the **Configure** tab.
5. In the **Device Option** list scroll to and click **User Authentication**.
6. Change **Setting** to **ON (Enhanced Server)** (for older devices, it is the **ON (Device)** option) and click **Apply**.



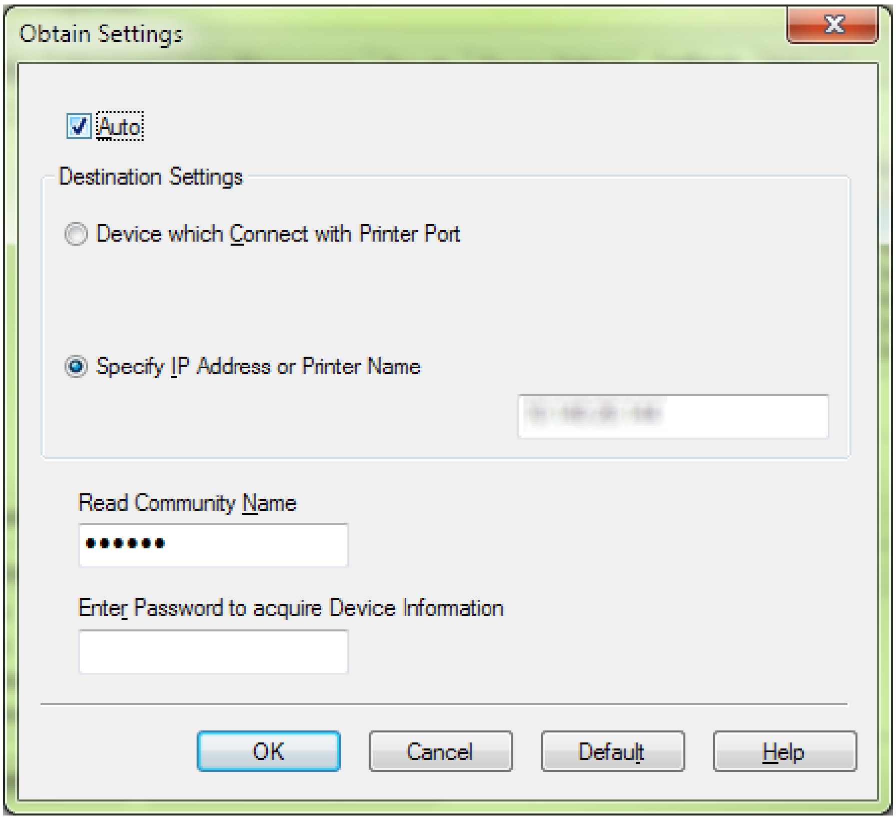
1200dpi Rendering Op.	None
Single Sign-On	Disable
User Authentication	ON (Enhance...
Public User	Restrict
Account Track	Disable
Wireless LAN	None
Extended Network(Operation Mode)	Do Not Use
Extended Network(Awake from ErP)	Do Not Awake

Setting: ON (Enhanced Server)

Disable
ON (MFP)
ON (External Server)
ON (MFP) + ON (External Server)
ON (Enhanced Server)
ON (MFP) + ON (Enhanced Server)

Tray	Size	Direction	Paper Type
Tray1	A4	SEF	Plain Paper
Tray2	A4	LEF	Plain Paper
Tray3	Unknown	Unknown	Unknown
Tray4	Unknown	Unknown	Unknown

7. Click **Obtain Settings** and **Specify IP Address or Printer Name**.



Obtain Settings

☑ Auto

Destination Settings

○ Device which Connect with Printer Port

● Specify IP Address or Printer Name

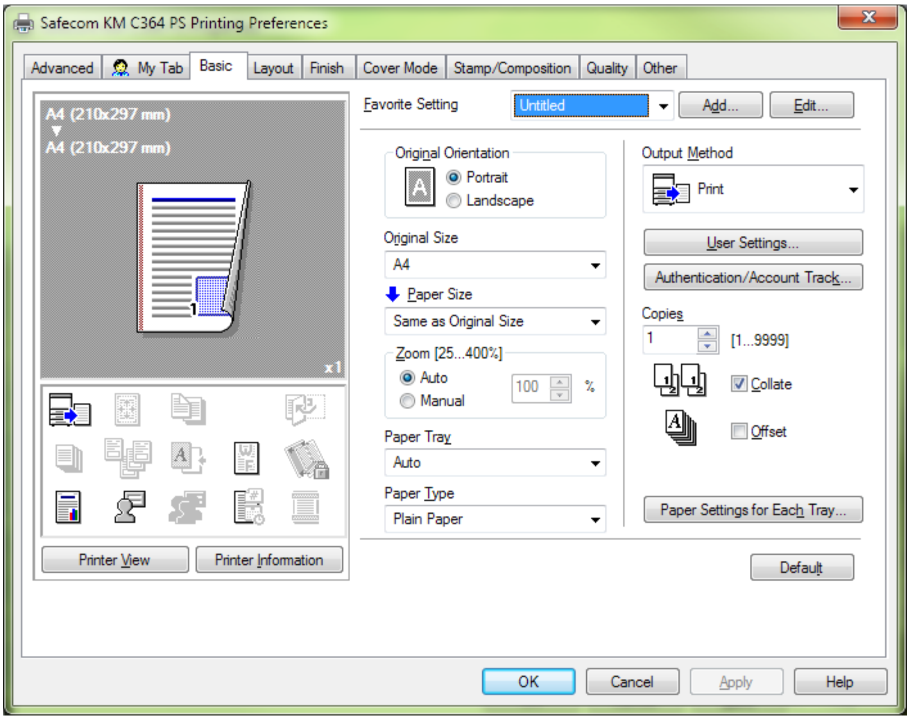
[redacted]

Read Community Name

••••••

Enter Password to acquire Device Information

8. Click **OK**, then click **Apply** on the **Configure** tab.
9. Click on the **General** tab and select **Printing Preferences.**
10. On the **Basic** tab click **Authentication/Account Track.**



Safecom KM C364 PS Printing Preferences

A4 (210x297 mm)
A4 (210x297 mm)

Favorite Setting: Untitled

Original Orientation: ● Portrait ○ Landscape

Original Size: A4

Paper Size: Same as Original Size

Zoom [25...400%]: ● Auto ○ Manual 100 %

Paper Tray: Auto

Paper Type: Plain Paper

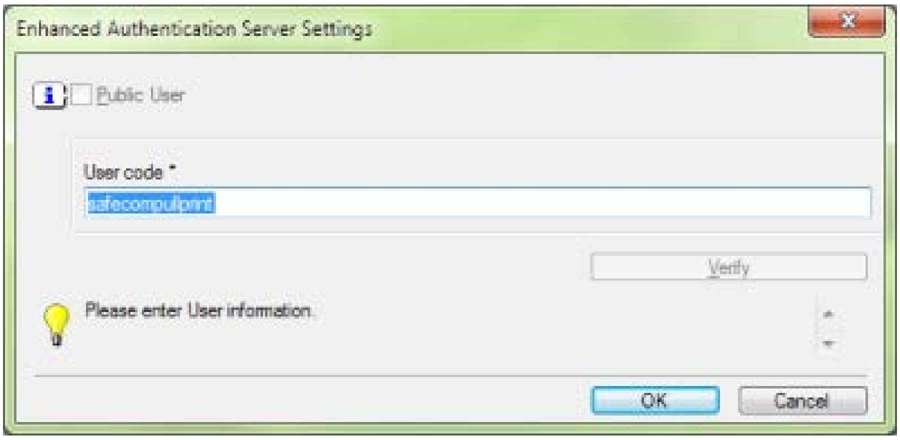
Output Method: Print

Copies: 1 [1...9999]

☑ Collate

□ Offset

11. Ensure that the **Public User** checkbox is cleared, set the **User code** to **safecompullprint**, then click **OK**.



safecompullprint

Please enter User information.

12. Go back to **Obtain settings** via the **Configure** tab and change the **Destination Settings** to **Device which Connect with Printer Port**.
13. Click **OK**.
14. On the **Configure** tab, click **Apply**, then **OK**.

At the device: ADF paper jam

If there is a paper jam on the ADF during copying, you must restart the whole process again. Tracking data from the jammed job is lost.

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 error message: “Unable to configure device because: Device does not appear to have SSL enabled.”

On some old device models, adding the device to the Device Server via SSL may fail due to the Java8 security restrictions, resulting in the above error message. In such cases, do the following:

1. Open the `<DS installation folder>\bin\jre\lib\security\java.security` file to edit.

2. Change `jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024`

   to

   `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024, DHE, ECDHE, ECDHE_RSA, DiffieHellman`.

3. Comment out the `jdk.tls.legacyAlgorithms= \ ...` lines.

Device freezes during logout while embedded web browser is starting

If your device is configured to automatically start the embedded web browser after login, do not log out before the web browser starts.

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 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.