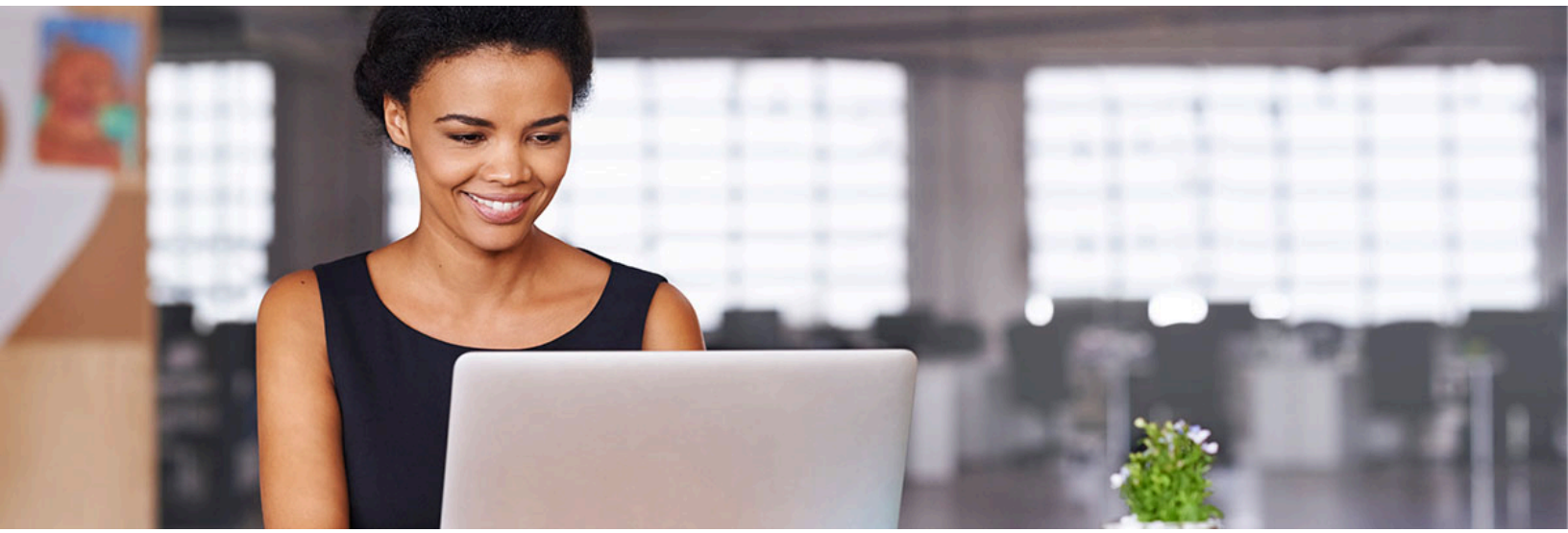


Kofax SafeCom Go Konica Minolta
Administrator's Guide

Version: 9.13.0

Date: 2021-11-15

KOFAX

Table of Contents

Preface

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

Getting help with Kofax products

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

To access the Kofax Knowledge Base:

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

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

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details, and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:

- Access the Kofax Community (for all customers).

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

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

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

Training

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

Chapter 1

Introduction

SafeCom Go Konica Minolta

SafeCom Go Konica Minolta is a solution for Konica Minolta MFPs. It integrates with the touchscreen 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.

SafeCom 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 the ID device.

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.

Chapter 2

Prepare the MFP

Prepare the MFP as follows:

- Allow the 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.

- The instructions below may vary between the different models. If you are in doubt, 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.

Open API settings

1. On the MFP's touchscreen 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).

Ensure 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

For enabling SSL certificate on Konica xx50 devices, follow the instructions in Enable SSL certificate on Konica xx50 devices. For other devices, do the following:

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**, select **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**.

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

Enable SSL certificate on Konica xx50 devices

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 touchscreen press the **Utility/Counter** button.
2. Tap **Administrator Settings**.
3. Enter the **AdministratorPassword**.

4. Tap **OK**.
5. Tap **User Authentication / Account Track**.
6. Set **Print without Authentication** to **Allow**.
7. Tap **OK** and restart the MFP.

Configure driver

Bizhub C35

ℹ 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**
4. In the **Setting** list, select **On (Enhanced Server)**.
5. Click the **Acquire Settings** button.
6. 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**.
7. In the **KONICA MINOLTA bizhub C35 Properties** window, click **Apply** then go to the **General** tab and click the **Preferences...** button.
8. In the **KONICA MINOLTA bizhub C35 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 **KONICA MINOLTA bizhub C35 Printing Preferences** window, click **Apply** and then **OK**.
12. In the **KONICA MINOLTA bizhub C35 Properties** window, click **OK**.

ℹ 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.

Bizhub C284e and C654e

ℹ 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** list to select the device model.
4. Select **User Authentication**, then in the **Setting** list select **On (Enhanced Server)**.
5. Click the **Obtain Settings** button.
6. In the **Obtain Settings** window, clear the **Auto** box, select **Specify IP Address or Printer Name** and type in the device IP address manually.
7. Click **OK**.
8. In the **KONICA MINOLTA <devicemodel> Properties** window, click **Apply**.
9. Go to the **General** tab and click the **Printing Preferences...** button.
10. In the **Printing Preferences** window, go to the **Basic** tab and click **Authentication/Account Track**.
11. In the **Enhanced Authentication Server Settings** window, remove the clear the **Public User** box.
12. In **User Code** type in anything. Do not click **Verify** as it will not work. Click **OK**.
13. In the **Printing Preferences** window, click **Apply**.
14. Click **OK**.
15. In the **Properties** window, click **OK**.

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.

Chapter 3

Safecom Go Konica Minolta

Overview

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

ℹ The MFP must be prepared so it allows use of OpenAPI, SSL on port number 50003, and print without authentication. For more information, see Prepare the MFP.

Install SafeCom Device Server

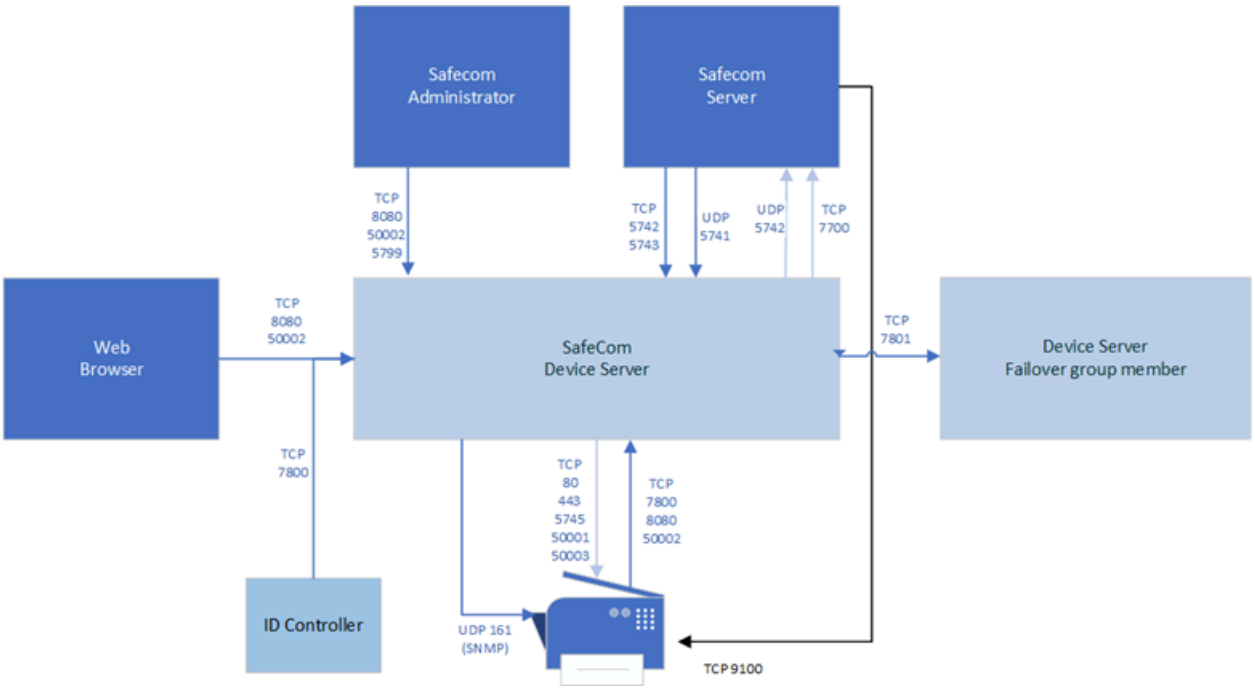
1. Download the SafeCom_Device_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be **Run as administrator**.
2. When the installation program is launched, click **Next**.
3. Select the destination folder for the files. Click **Next**.
   The default installation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

Windows firewall – Ports that must be opened

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

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

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



Inbound connections

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

Outbound connections

161	SNMP (UDP)	Device discovery
443	HTTPS	Used to contact MFP during operation
5742	UDP	SafeCom identification (SafeCom G4 Server / Broadcast Server)
5745	TCP	HP Jedi call back
7627	HTTP	HP Jedi Web services (unsecure)
7700	TCP	SafeCom Server (Job Server), Configurable to 7500 Protocol: • Version 9.13 and later - Configurable TLS 1.2 or SafeCom • Versions earlier than 9.13 – SafeCom
7801	TCP (RAW)	Failover: data exchange
50001	HTTPS	MFP
50003	HTTPS	MFP (Konica Minolta)

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

Configure SafeCom Device Server

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

Log in to SafeCom Device Server

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

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

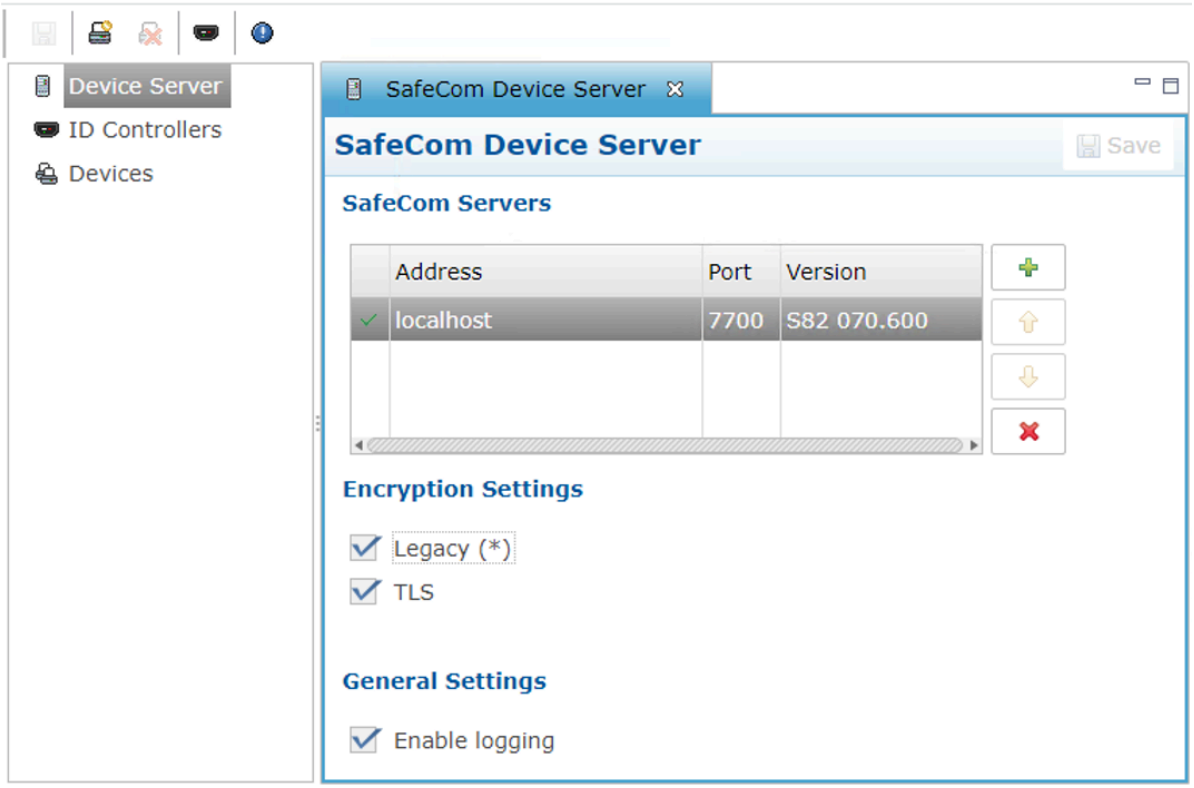
   Example https://localhost:50002/safecom

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

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

Add SafeCom Server

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



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

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

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

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

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

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

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

6. Optionally, you can enable the Device Server logging feature for diagnostic purposes.
7. When all settings are configured, click **Save**.

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

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

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

Device Server config.ini

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

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

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

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

Add device to the SafeCom Device Server

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

- Through the SafeCom Administrator:

  This is the recommended method and it works for SafeCom G3 Server version S82 070.410*05 or higher.
- Through the SafeCom Device Server:

  Solutions based on SafeCom G2 must use this method.

Device icons

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

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

Add device through the SafeCom Administrator

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

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

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

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

Add a device server device

1. Click the **Devices** container, right-click the content area and select **Add device**.
   The Add Device Wizard appears.
2. From the **Device server** menu, select the **SafeCom Device Server** and click **Next**.
   Information is retrieved from the device server to establish the status of the device server.
3. Click **Next**.
4. Enter the **Printer address** (the device IP address or host name) and click **Next**.
   Information is retrieved from the device.
5. Click **Next**.
6. Select **SafeCom Go Konica Minolta** as the type of device and click **Next**.
7. Enter the username and password as specified on the device web page, then click **Next**.
   The device properties dialog box opens.
8. Make sure to specify on the **Settings** tab the device server and the capabilities of the device.

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

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

   The device server device is now added and listed both under **Devices** and under the device server under **Device servers** with the name SafeCom Device Server.
10. Go to the Configure device in SafeCom Device Server section to continue with the configuration of the device.

Add device through the SafeCom Device Server

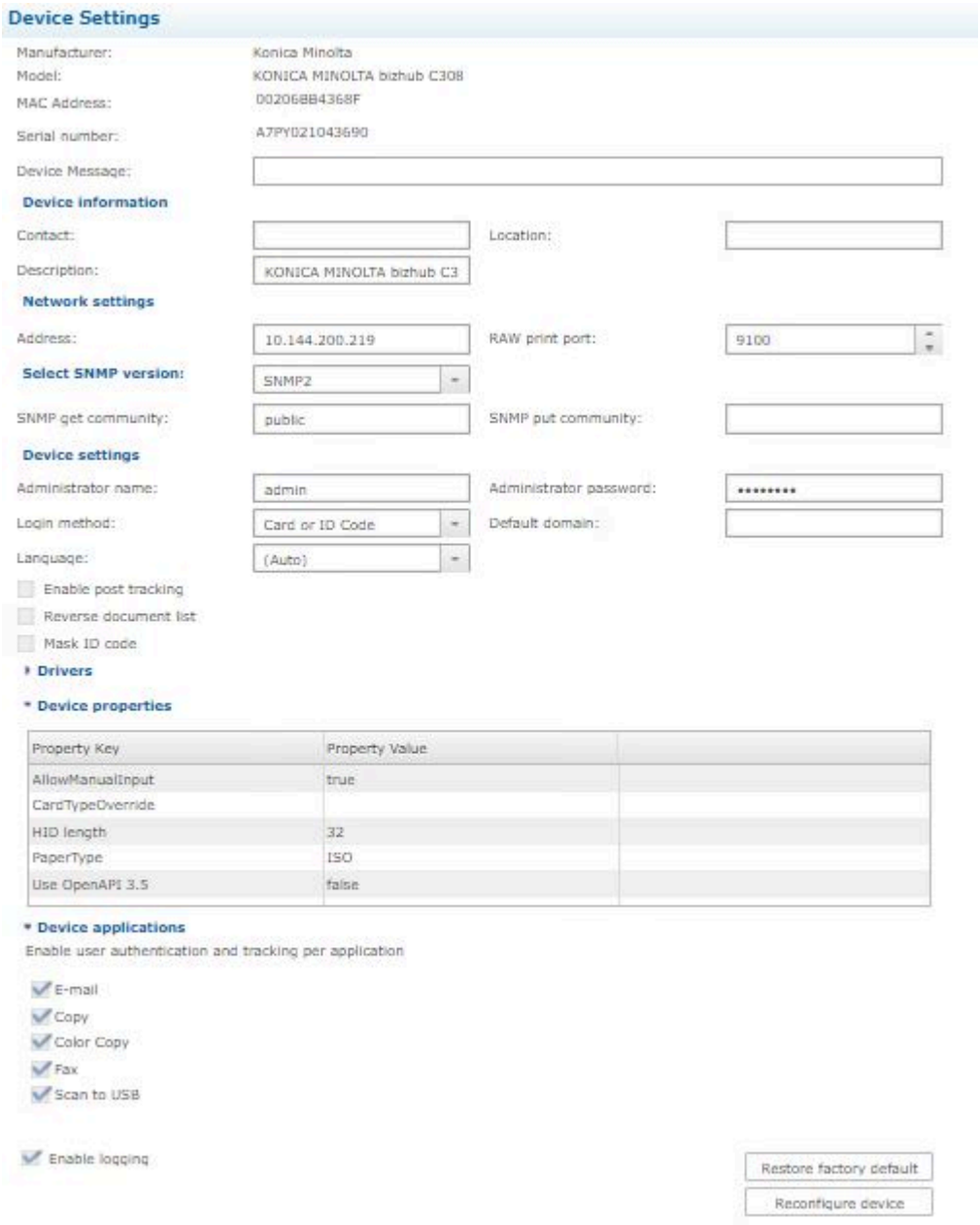
1. Click **Device Server** in the left menu.
2. Click the **Add device** button.
   The Add Device Wizard appears.
3. Enter the hostname or the IP address of the device.
   If you want to use dynamic IP address, enter the device hostname in the **Address** field.
4. Enter the administrator name and password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

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

Configure device in SafeCom Device Server

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

If the configuration of the devices fails, it might be because the Device Server is installed on a server that has multiple NICs or IPs. See 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.

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

Change the settings according to the following descriptions:

Option	Description
Device information	• 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.
	• **Select SNMP version**: These properties must match the SNMP settings of the device. First, select the SNMP version configured on the device. The SNMP related fields change according to the selected version.
	  • **SNMP v2**: Provide SNMP Get and Put Community name. The default value of these properties is public.
	  • **SNMP v3**: Provide the **Username**, select the **Authentication** protocol and enter the **passphrase**, select **Privacy Protocol** and enter the **passphrase**

Device settings	• Administrator name: The user name with which the administrator can log in to device.
	• Administrator password (mandatory): The device password with which the administrator can log in to device.
	• Login method: This determines how users log in. Select one of the following:
	  • 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.
	
	  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.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>

Language: Specify a specific language if you want SafeCom Device Server to override the language on the device.
Hide domain: This option can be used if you specified a default domain. Check it to allow the users to log in without typing in the domain.
Enable post tracking: This option is relevant only with SafeCom Tracking. For more information, see the SafeCom G4 Administrator's Manual.
Reverse document list: Check this option to show the first printed documents at the top of the document list.

</td></tr>
<tr><td>Drivers</td><td>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.</td></tr>
<tr><td>Device Properties</td><td>

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.
<table>
<tr><th>Property value</th><th>Description</th></tr>
<tr><td>FELICA_IDM</td><td>Felica</td></tr>
<tr><td>TYPE_A</td><td>MiFare</td></tr>
<tr><td>HID_PROX</td><td>HID</td></tr>
<tr><td>MAGNETIC_CARD</td><td>Magnetic</td></tr>
</table>

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.

</td></tr>
<tr><td>Device applications</td><td>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 boxes are selected. the welcome screen only shows the option to Login and Windows login if enabled.</td></tr>
<tr><td>Enable logging</td><td>Select this option if log information should be collected.</td></tr>
</table>

Option	Description
	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 if instructed by SafeComSupport. If the device is unable to upload to the server, the device will keep the log and try to upload again after another hour. ℹ The device will always log performance data (network latency, authentication duration of successful logins, number of Out of order occurrences and duration, failover and failback between G4 servers, device reboots, changes in firmware and Go versions).
Restore factory default	This button sets all settings to their default value except from the password.
Reconfigure device	This button references the device to the current SafeCom Device Server.

Use Safecom Go Konica Minolta

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. For example, if the device has a card reader installed, you must change the Login method to a method that includes a card.

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

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**.

ℹ 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".

ℹ 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.

Follow these steps to enable post tracking for the device.

1. Log in to **SafeCom Device Server**.
2. Expand **Device Server** in the left pane 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, click **User Authentication**.
3. Change **Setting** to **ON (Device)** and click **Apply**.
4. Click on the **General** tab and select **Printing Preferences**.
5. On the **Basic** tab, click **Authentication/Account Track**.
6. Select **Recipient User** and enter username as **safecompullprint** and click **OK**.

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. Make the appropriate changes on the **Settings** tab. In particular, make sure that **Duplex supported** and **Color supported** is set correctly.
6. Select the appropriate charging scheme on the **Charging scheme** tab.
7. Check the appropriate licenses on the **License** tab.
8. Click **OK**.

ℹ 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 Install SafeCom Device Server).

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.

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

1. Press the **Utility/Counter** button on the MFP.
2. Tap **Meter Count**.
3. Tap **Check Details**.
4. Press the **Stop** button.
5. Enter 00 (zero zero) on the keypad.
6. Press the **Stop** button.
7. Enter 01 (zero one) on the keypad.
8. Press the **Stop** button.
9. Enter 9 (nine) on the keypad.
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 off the device.
    Wait 10 seconds or more before turning the power on again.

ℹ Performing the above steps may change the ID & Print setting away from OFF. Please set it back to OFF.

Set ID & Print to OFF

1. Press the **Utility/Counter** button on the MFP.
2. Tap **Administrator Settings**.
3. Enter **Password**.
4. Tap **OK**.
5. Tap **User Authentication / Account Track**.
6. Tap **User Authentication Settings**.
7. Tap **Administrative Settings**.
8. Tap **ID & Print Settings**.
9. Set **ID & Print** to **OFF**.
10. Tap **OK**.

11. 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:

Through 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)**.

Through User registration

1. Press the **Function counter** button and then **Administrator settings**.
2. Enter the code '12345678'.
3. Select **User Authentication/Account track**.
4. 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. For more information, see the *SafeCom G4 Administator's Manual*. You can control access rights to the following features:

- Copy
- E-mail
- Scan
- Fax

ℹ 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 to uninstall the SafeCom Go solution.
3. Click the **Delete** icon in the top menu to uninstall.
4. Click **Save**.

Use SafeCom Go Konica Minolta device trace facility

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

Enable SafeCom trace facility through the configuration web page

The SafeCom trace facility is enabled through the configuration web page. It is used for troubleshooting.

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.

Enable SafeCom trace facility through the SafeCom Device Server

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 **Logging enabled** box at the bottom of the page is selected.
3. Click **Save**.

See the trace files generated by the Device Server

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

   The default installation folder is:

   - On Windows 32-bit:

     `C:\Program Files\SafeCom\SafeCom Device Server\logs`
   - On Windows 64-bit:

     `C:\Program Files (x86)\SafeCom\SafeCom Device Server\logs`
2. If you need to send the log files, make sure to save and send the folder logs as a compressed/zipped folder.

Configure the trace files

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

1. Browse to the config.ini file:
   - On Windows 32-bit:

     `C:\Program Files\SafeCom\SafeCom Device Server\equinox\config.ini`
   - On Windows 64-bit:

     `C:\Program Files (x86)\SafeCom\SafeCom Device Server\equinox\config.ini`

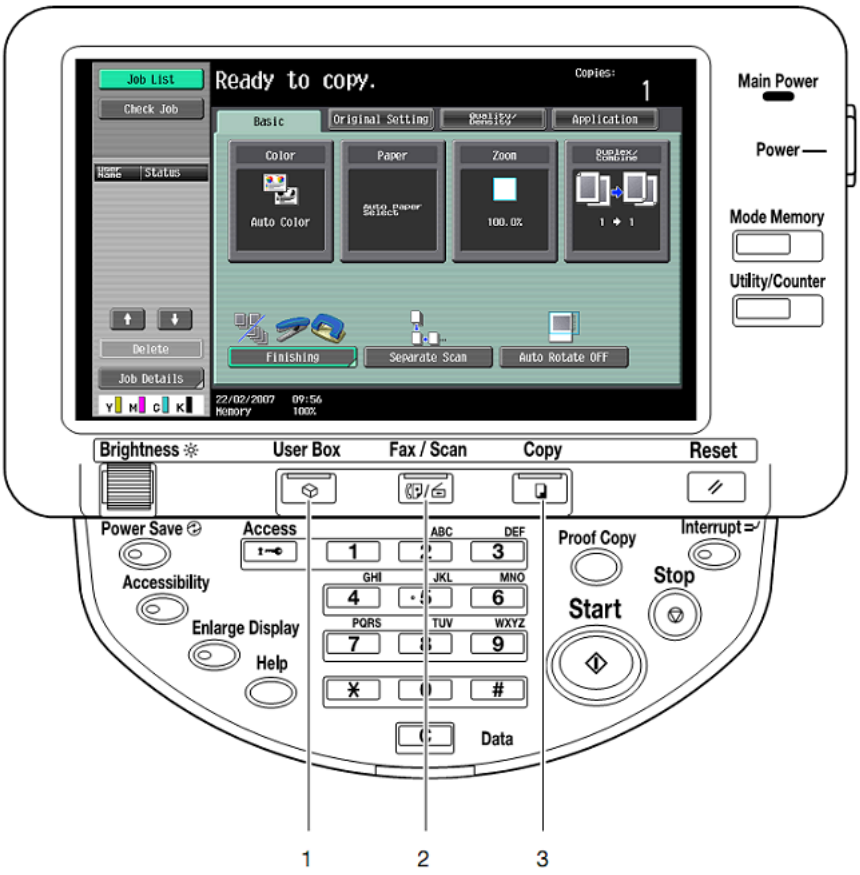
2. Double-click the config.ini file. In the opened file, scroll to the bottom and add:
   - `deviceserver.trace.file.size` – to configure file size. Size is written as a number with an optional qualifier. For example: ten is 10 bytes, ten kilobytes is 10KB, ten megabytes is 10MB, and one gigabyte is 1GB.
   - `deviceserver.trace.file.count` – to configure how many trace files are generated. Enter the number of files you want to generate as a number.

After configuring the trace files, restart the SafeCom service.

Chapter 4

Using Safecom Go Konica Minolta

Control panel



Login

Log in with card

Use card reader.

Log in with card and PIN code

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

Log in with ID code

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

Log in with Windows

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

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

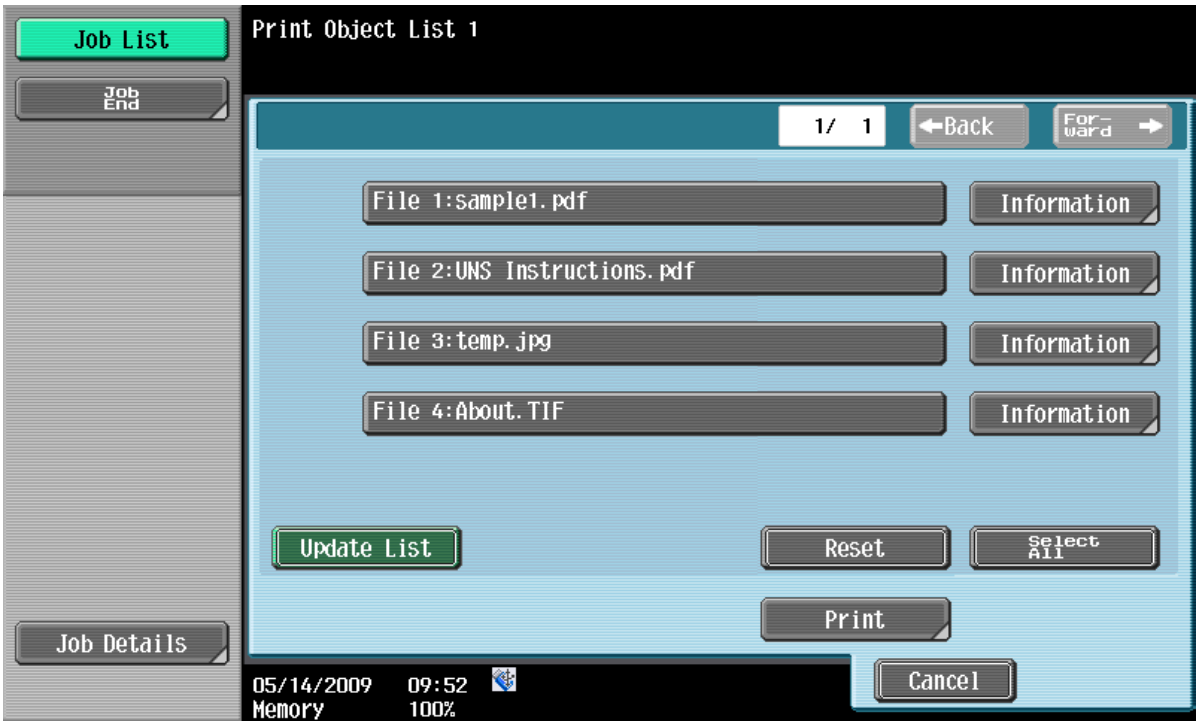
Username and Password cannot be blank.

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.

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 documents.
   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.



The document list looks 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).

Send e-mail

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

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

Logout

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

Press the **Access** button  to log out.

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 prompted to enter his PUK code.
2. Tap **PUK code** on the touchscreen.
3. Enter **PUK code** and tap **OK**.
4. Tap **PIN code** on the touchscreen.
5. Enter **PIN code** and tap **OK**.

The card is registered and you are asked to log in again.

Chapter 5

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 troubleshooting hints.

Servlets

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

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

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

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

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

SafeCom Device Server does not start

Ensure that your Java Runtime Environment is working properly.

Authentication Version 2.0 Not Found

If you see the "Authentication version 2.0 not found" error message 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

Follow these steps to change software switch settings:

1. Press the **Function Counter** button on the device.
2. Tap the **Meter Count** button on the display and then **Check details**.
3. Enter the Service mode by pressing the **Stop** button.
4. Enter '00'.
5. Press **Stop** button again.
6. Enter then '01'.
7. In the service mode, tap **System 2**.
8. Tap **Software Switch Settings**.
9. Type '25' in **Switch No.** field.
10. Type '20' in **Hex Assignment** field.
11. 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 have to reconfigure your device properties due to device-specific User Authentication naming.

1. Log in to **SafeCom Device Server**.
2. Expand **Device Server** in the left pane 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. Click **User Authentication** in the **Device Option** list.
6. Change **Setting** to **ON (Enhanced Server)** and click **Apply**.
   On older devices, this option is called **ON (Device)**.
7. Click **Obtain Settings** and **Specify IP Address or Printer Name**.
8. Click **OK**
9. Click **Apply** on the **Configure** tab.
10. Click on the **General** tab and select **Printing Preferences**.
11. Click **Authentication/Account Track** on the **Basic** tab.
12. Ensure that the **Public User** check box is cleared.
13. Set the **User code** to **safecompullprint**, then click **OK**.
14. Go back to **Obtain settings** through the **Configure** tab.
15. Change the **Destination Settings** to **Device which Connect with Printer Port**.
16. Click **OK**.
17. On the **Configure** tab, click **Apply**, then click **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. For more information, see Device Server config.ini.

Device Server: Error when upgrading existing device server installation

The "Error in action StopWindowsService" error might appear when upgrading an existing Device Server installation:

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 through 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 following line:
   `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.

Chapter 6

Regulatory information

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

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

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

CAUTION: Changes or modifications not expressly approved by Kofax, Inc. could void the user’s authority to operate this equipment according to part 15 of the FCC rules.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to take whatever measures may be required to correct the interference at the user's own expense.

CE conformance: This product has been developed and produced in accordance with the EMC directive and the Low Voltage directive and therefore carries the CE mark.

EMC directive: This product observes the rules and regulations of the EMC directive. If so required, a declaration of conformity in local language stipulating the applied rules and regulations can be obtained.