PaperCut MF - Konica Minolta Standard UI Embedded Manual

Contents

1 Document revision history

Published date or release	Details of changes made
19.1.0	3 Installation
18.3.6	7.3 Configuring Swipe Card Readers; 7.1 Config Editor
18.3.0	7.1 Config Editor

This manual covers the PaperCut MF Konica Minolta embedded setup. For general PaperCut MF documentation, please see the PaperCut MF manual.

2 Installation

This section covers the installation of the PaperCut embedded application for compatible Konica Minolta devices. The embedded application will allow the control, logging and monitoring of walk-up off-the-glass copier usage and may serve as a print release station for network prints (for information on just tracking network printing see the PaperCut user manual).

2.1 Supported devices

PaperCut MF supports any multi-function Konica Minolta device with "OpenAPI" functionality, a hard drive installed, a compatible web browser, and listed as a supported device on the PaperCut MF for Konica Minolta page.

PaperCut MF requires OpenAPI version 2.3.1 or higher with version 3.1 or later recommended. This is because devices with OpenAPI 3.1 or later provide additional comfort during the login and account selection process, allowing users to self-associate a swipe card with their existing account and provide more precise accounting and zero-stop while using the copier functions.

Device type in PaperCut MF	i-Option UI Supported?	Standard UI Supported?
Konica Minolta (OpenAPI 2.3+)	No	Yes
Konica Minolta (OpenAPI 3.1+)	Yes • OpenAPI 3 and OpenAPI 4 devices with a hard drive installed. • LK101 upgrade kit may be required from Konica Minolta • A web browser (depending on MFP model)	Yes • OpenAPI 3 and OpenAPI 4 devices with a hard drive installed
Konica Minolta (OpenAPI 4.0+)	Yes • OpenAPI 3 and OpenAPI 4 devices with a hard drive installed. • LK101 upgrade kit may be required from Konica Minolta • A web browser (depending on MFP model)	Yes • OpenAPI 4 devices with a hard drive installed

NOTES:

- Production devices offer a more limited version of the UI than other standard UI devices. All Production Printing (PP) models must use the IC602 controller.

- Some older devices also require additional memory when running OpenAPI applications (like PaperCut). Many older devices can have their firmware upgraded to support version 3.1/4.0.

2.2 Requirements

Before installing the PaperCut Embedded Application into the Konica Minolta device, ensure that basic monitoring of network printing has been setup up and tested for this device. The device would show up in the printer list in the PaperCut web interface and have a few print jobs in its print history.

After that, ensure that the following points are checked off before getting started:

- PaperCut is installed and running on your network. Please see the 'Introduction -> Quick Start Guide' section of the PaperCut user manual for assistance.
- Ensure that your Konica-Minolta device supports OpenAPI 2.3.1 or later with OpenAPI 3.1 or later is recommended.
- Ensure that the Konica Minolta device is connected to the network.
- Have available the network name or IP address of Konica-Minolta device.
- It is recommended that the device be configured with a *static IP address*.
- Verify that firewalls or other network restrictions don't prevent the PaperCut server's access to port 50003 on the device and don't prevent the device's access to the PaperCut server on ports 9191 and 9192.

2.3 Setup Procedure

2.3.1 Configure OpenAPI Settings

- Log on as administrator onto the device's web interface (called "Page Scope Web Connection") under http:// <ip-address-of-device>/ .
- In the "Security" section display the "PKI Settings" subsection. If there is no "PKI Settings" subsection, please ignore this section and refer to Appendix A instead for configuration of older devices.
- Create a new certificate following these steps. (Even if a certificate is already shown in the "Device Certificate List", this certificate may not be usable for SSL. Please delete it and re-create a new one.)
    - Click "New Registration", select "Create and register a self-signed Certificate" and click "OK".
    - Fill in the fields with some values about your organization. The values have no functional significance.
    - For the Validity Period the maximum number of days offered is recommended (usually 3650 = 10 years).
    - "Encryption Strength" can be left to the default values.
    - Click OK. The certificate will be generated. You will be asked to switch the device off and on again.
- Log onto the device web interface as administrator again and in the "Security" section display the "PKI Settings" subsection and from the menu on the left choose "SSL Setting". Change "Mode using SSL/TLS" to "Admin Mode" or "Admin Mode and User Mode" (on some machines: just "enable"). Your web browser will re-logon to

the web server under “https” mode. You may have to confirm an “invalid certificate” in your browser.

- Optionally, if you are still using the default password, please change it in the “Security” section display the subsection “Administrator Password Settings”, tick “Password is changed” and enter a new password and click “OK”. Remember this or keep it in a safe place.
- In the “Network” section, display the subsection “TCP Socket Setting”. Tick “Use SSL/TLS” and click “OK”. You will be asked to switch the device off and on again.
- Log back into the administrator web interface, and in the “Network” section display the “OpenAPI” subsection.
    - From the “Use SSL/TLS” drop-down list select “SSL Only”.
    - Make sure the “Port No. (SSL)” is set to 50003.
    - All “Certificate Verification Level Settings” should be set to “Do not request” (1st item) or “Do Not Confirm” (all other items), including “Validity Period” which often is set to “Confirm” by default.
    - Click OK.
- Some newer devices, an OpenAPI password has been set that needs to be removed. To do so, access the administrator settings on the device’s panel (not in the web interface):
    - Press the “Utility” button on the button panel.
    - Press “Administrator Settings” on the screen.
    - Log in with the administrator password.
    - Selection “System Connection” > “OpenAPI Settings” > “Authentication”.
    - Make sure “OFF” is selected and press “OK”.
- For security reasons it is recommended also change the device’s default administrator web access password.
- Ensure SSDP protocol is enabled under Utility > Administrator > Settings > Network Settings > SSDP Settings.

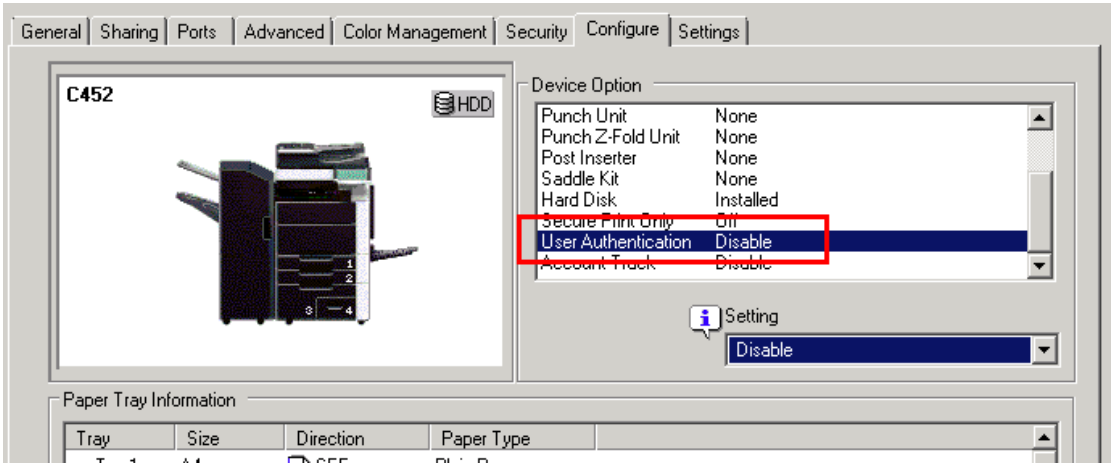
2.3.2 Enabling Unauthenticated Printing

When PaperCut is monitoring print queues it has control of what print jobs are allowed to print. If PaperCut allows a job to print, we do not want the Konica Minolta device to deny the print job, or track printing twice (duplicate charging). This requires that the print authentication is disabled in the printer driver and on the device as described below.

Set up a print queue for the Konica MFD on the print server using Konica’s print drivers. The driver has to be configured to allow unauthenticated printing. For Windows, right-click the corresponding printer icon in the Printers section of Windows Control Panel and select “Properties”. Select the “Configure” tab and:

- Click “Acquire Settings”. Make sure the “Auto” check box is **not** selected. Click OK.
    - NOTE: On some newer models, the “Auto” check box can only be unchecked and saved if the IP address and device administrator password are entered, because the setting is saved on the copier.

- At the top right of the “Configure” tab, in the Device Options list, scroll down to “User Authentication” and select “Disable”.



- Close the Properties window by clicking OK.

For other operating systems, please consult your Konica documentation.

NOTE: If you are using a virtual queue for load balancing/”find me” printing, apply that same setting to the virtual queue, too.

In addition, a corresponding device option has to be set on the device, either on the device screen or in the device web interface. Some devices may not offer the option to configure at the device or in the web interface. For configuration at the device screen:

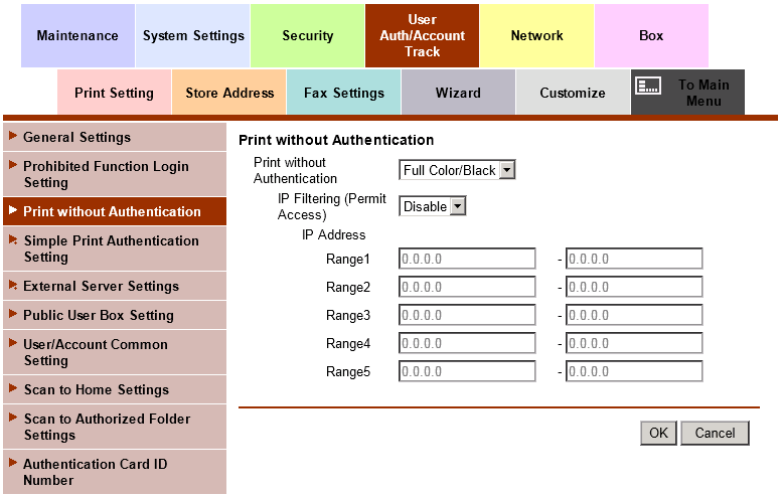
- Press the “Utility/Counter” button.
- Select “Administrator Settings”. Enter your administrator password and press OK. (The default administrator password on Konica devices can be found in the Konica Minolta manual.)
- Select “User Authentication/Account Track”.
- Select “Print without Authentication”.
- Select “Allow”.
- Select “OK”.

For configuration via the web interface:

- Open the device’s IP address or hostname in a web browser.
- Log in as the Administrator.
- Select Security -> Authentication -> General Settings.
- Set “Public Access” to “Restrict”.
- Set “Print without Authentication” to “Allow”.
- Select “Apply”.

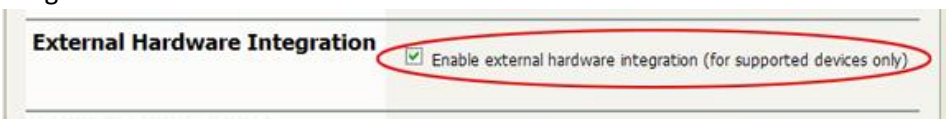
Alternatively, on some copiers it’s found via:

- Open the device’s IP address or hostname in a web browser.
- Log in as the Administrator.
- Select User/Auth/Account Track.
- Select Print without Authentication
- Set “Print without Authentication” to “Full Color/Black”

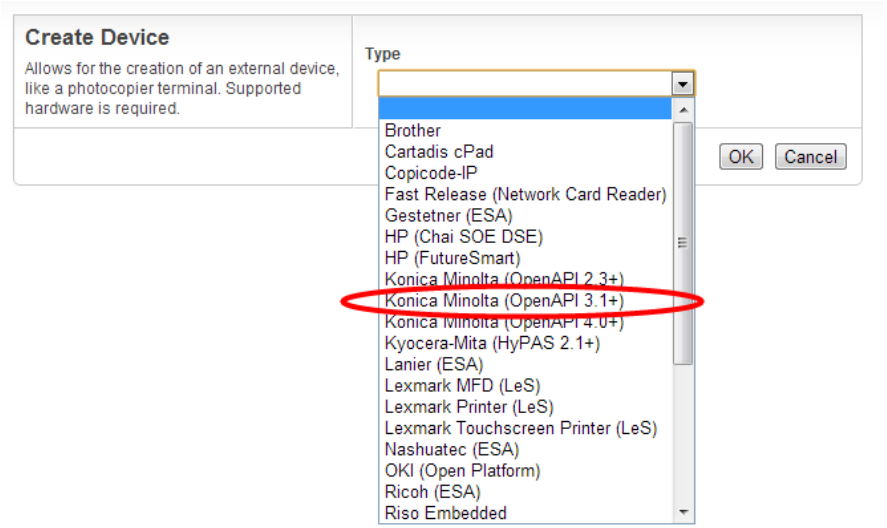


2.3.3 PaperCut Settings

1. Ensure that you are logged out of the device's web interface from the previous step. PaperCut cannot communicate with the device while an administrator is logged into the device's web interface.
2. Log in to the PaperCut administration interface using a web browser (e.g. http://papercut-server:9191/admin).
3. Navigate to 'Options -> Advanced' and ensure the option 'Enable external hardware integration' is enabled.



4. Press 'Apply'.
5. Navigate to the 'Devices' tab.
6. Click "Create Device".
7. Enter a descriptive name for the device under "Device name".
8. Enter the device's network name or IP address under "Hostname/IP".
9. Optionally enter location/department information.
10. From the "Type" drop down, select the Konica Minolta OpenAPI version supported by your device.



11. Enter "Admin" as the administrator username and enter the password set in step 2.3.1.
12. Under “Function” tick “Track & control copying” and “Enable print release”. Enabling both copy and print release functionality allows for post-installation testing. Chapter 4 shows how to change this setting later.
13. Click “OK”.

The “Device Details” screen will now show and it has an area titled “Device status” which after clicking the “Refresh” link should show “Started – setting up device integration…”. Please click “Refresh” again a few times until the status field shows “Started - connection confirmed”.

At the same time, the screen on the device should first go blank with a message “Now remote operating” and after 10-15 seconds should show the “Authentication” screen with username and password field.

You should now proceed to configure page costs and other settings relating to the device.

2.3.4 Additional Network Security (optional)

The MFP communicates with the PaperCut server over the network (e.g. to authenticate users or release print jobs). To provide an additional level of security, PaperCut may be configured to only allow device connections from a restricted range of network addresses. This ensures that only approved devices are connected to the PaperCut server.

By default, PaperCut will allow device connections from any network address. To restrict this to a subset of IP addresses or subnets:

1. Logon to the PaperCut administration web interface at http://<papercut-server>:9191/admin
2. Go to the Options→Advanced tab and find the “Security” section.
3. In the “Allowed device IP addresses” field enter a comma-separated list of device IP addresses or subnets (in the format <ip-address>/<subnet-mask>).
4. Press the “Apply” button.
5. Test the devices to ensure they can continue to contact the PaperCut server.

2.4 Upgrading to a newer version

The embedded application will be up to date when you upgrade your PaperCut installation, no further action is necessary.

3 Post-install testing

After completing installation and basic configuration it is recommended to perform some testing of the common usage scenarios. This important for two reasons:

1. To ensure that the embedded application is working as expected
2. To familiarize yourself with the features and functionality of PaperCut and the embedded application.

This section outlines four test scenarios that are applicable for most organizations. Please complete all the test scenarios relevant for your site.

The following test cases assume a device with OpenAPI 3.1 or later. Due to restrictions in earlier versions of OpenAPI (2.3 or later), some restrictions apply during log in and account selection. Please see Appendix A for guidance on using older systems.

3.1 Test Preparation

To complete these tests, it is recommended you use two test users so that each can be configured differently. These users are:

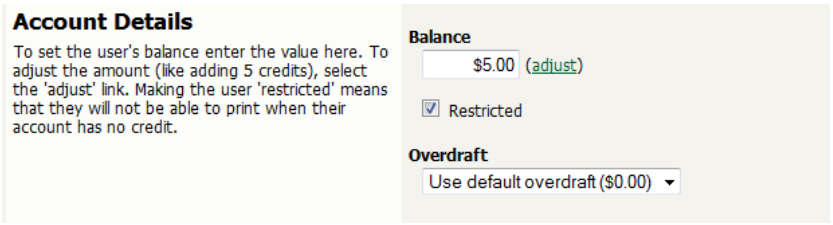
- 'testusersimple' – is used to perform basic copier monitoring and control and to perform print release tests.
- 'testuseradvanced' – is used to perform copier monitoring and control with the account selection enabled (i.e. to charge copying to accounts/departments/cost-centers/etc).

To setup these users in PaperCut:

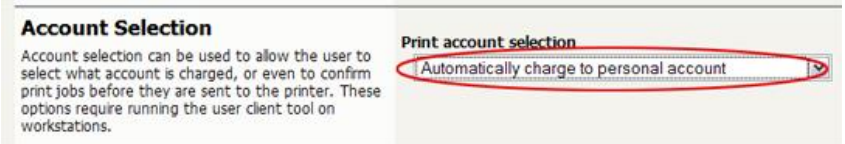
1. Create the 'testusersimple' and 'testuseradvanced' users in your Active Directory or LDAP directory.
2. Login to the PaperCut's admin web interface
3. Go to the "Options->User/Group sync" page and press "Synchronize Now".
4. Once the sync is complete, the users will be added to PaperCut.

The next step is to configure the users. To configure 'testusersimple':

1. In PaperCut, select the "Users" tab
2. Select the 'testusersimple' user.
3. Set the user's balance to $5.00 and verify the account is set to "Restricted".



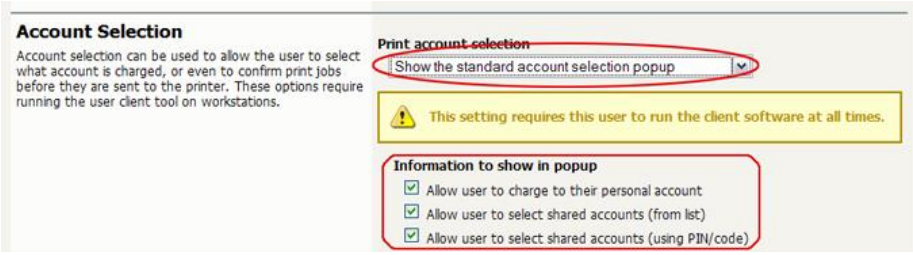
4. Verify that this user is set to "Automatically charge to personal account" in the "Account selection" options.



5. Press the “OK” button to save.

To configure ‘testuseradvanced’:

1. In PaperCut, select the “Users” tab
2. Select the ‘testuseradvanced’ user.
3. Change the “Account Selection” option to “Standard account selection popup” and enable all the account selection options.



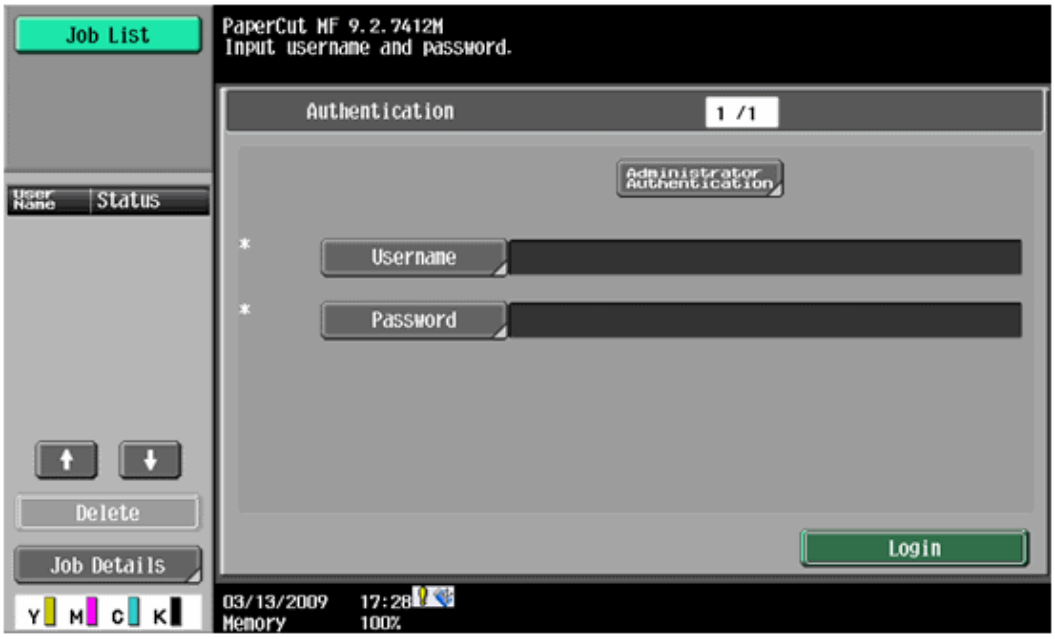
4. Press the “OK” button to save.

3.2 Scenario 1: Standard copying

Standard copying involves monitoring/charging printing to a user’s personal account. This is the most commonly used for student printing or basic staff monitoring. Users can also be configured for unrestricted printing, which is commonly used for staff/employee use.

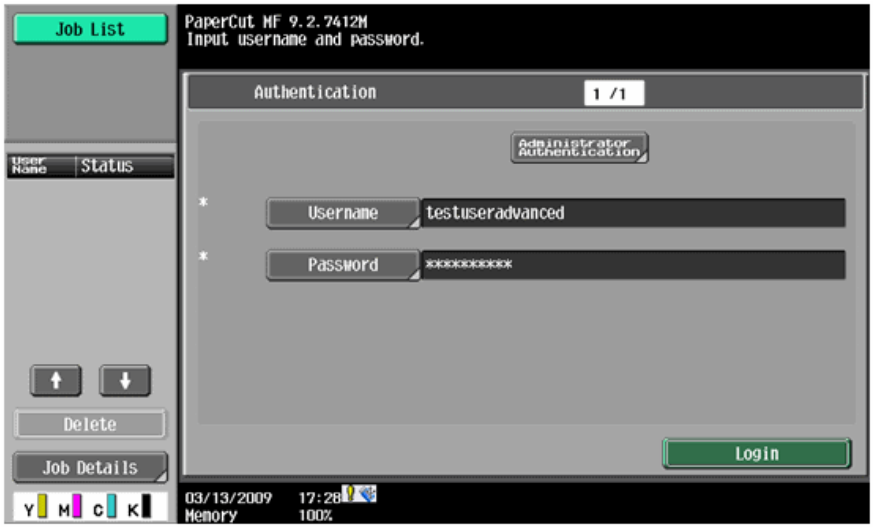
At the photocopier:

1. The photocopier should be showing the “Authentication” screen as shown below.



2. Press the “Username” button to the left of the first blank field, enter the username “testusersimple” using the on-screen keyboard and press “OK”. Likewise, press the “Password” button and enter the password previously chosen.

3. Your screen should now look like this, press “Login”.



4. The screen will now show a login confirmation:

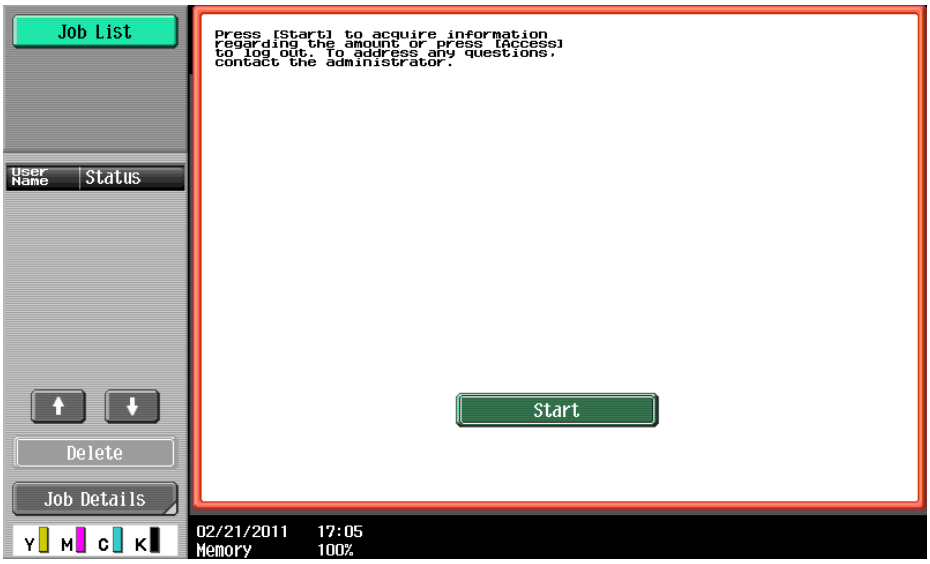
5. At this point the copier will be enabled for usage.
6. Follow the onscreen instructions and perform some test copying, i.e. press the “Start” button on the device button panel and perform a copy as normal.
7. Once completed copying press the “Access” button on the device’s button panel and confirm logging out by pressing “Yes” and “OK” on the screen.

Back in the PaperCut application verify that the copier activity was recorded and the user's account deducted.

1. Log in to PaperCut.
2. Select the device from the "Devices" tab.
3. Select the "Job log" tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed. Verify the details of the copy job that was just performed.

Usage Date	User	Charged To	Pages	Cost	Document Name	Attribs.
Apr 16, 2008 2:59:30 PM	testusersimple	testusersimple	2 (Color: 0)	$0.20	[copying]	A4 (ISO_A4) Duplex: No Grayscale: Yes

NOTE: If the user runs out of credit while copying, the following warning will be displayed:



At this point the user can only log out by pressing the "Access" button on the copier panel.

3.3 Scenario 2: Copying with account selection

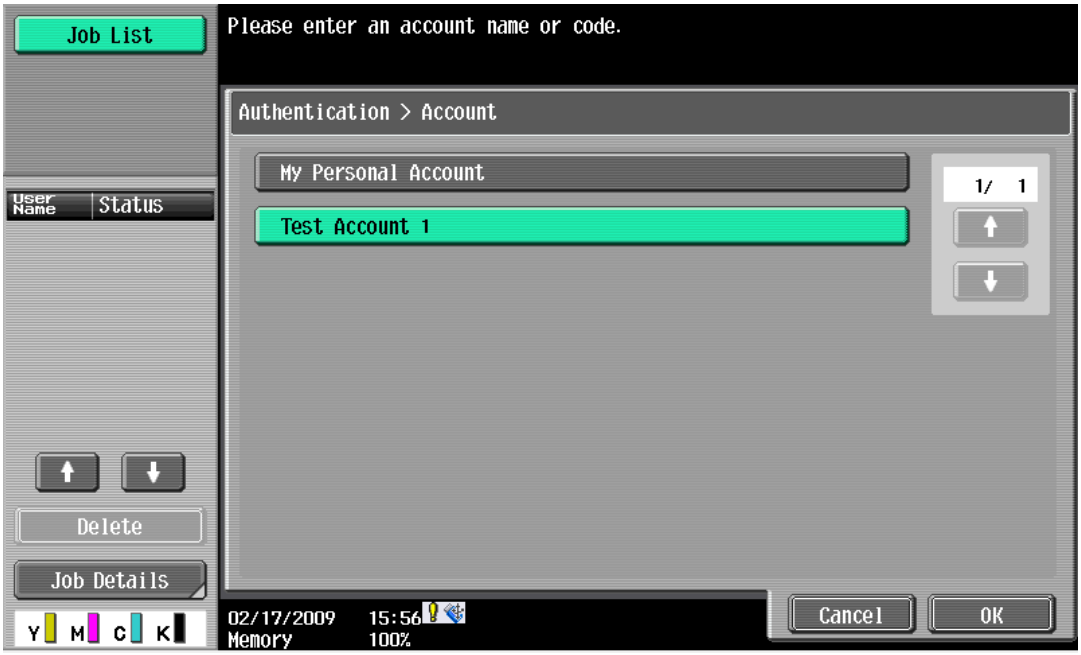
Firstly, a test account should be created:

1. Log into PaperCut, select the "Accounts" tab.
2. Select the "Create a new account…" action link on the left.
3. Enter an account name "Test Account 1".
4. Enter PIN/Code "2233".
5. Select the "Security" tab and allow all users to access that account by adding the "[All Users]" group.
6. Press "OK".

At the photocopier:

1. The photocopier should be showing the "Authentication" screen as before.
2. Enter the username ('testuseradvanced') and password as before and press "Login".
3. An account selection screen appears with two fields. Press the Account List button to the right of the account field. The account list will show after a brief moment.

4. Select “Test Account 1” by pressing the button, it will highlight in green. Press OK.



5. The screen will now show the Account field pre-filled with your selection. Press “OK”.
6. The confirmation screen will show that “Test Account 1” has been selected. Acknowledge by pressing “OK”.

7. Now perform copying as normal and finally log out using the “Access” button as before.

Back in the PaperCut application verify that the copier activity was recorded and the user’s account deducted.

1. Log in to PaperCut
2. Select the device from the “Devices” tab
3. Select the “Job log” tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed.
4. Verify the details of the job (i.e. that the job was charged to the selected account).
5. In the log details, click on the “Charged To” account name to view the account’s details.

6. Selecting the “Job log” tab will display all print/copy activity for the account, and will show the test photocopying that was performed.

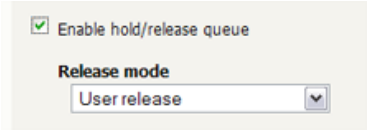
3.4 Scenario 3: Print release

The embedded application may also be used for print release. For full description of PaperCut hold/release queues and print release, please read the PaperCut manual.

Skip this scenario if hold/release queues will not be used at your site.

To perform print release testing a hold/release queue must be enabled:

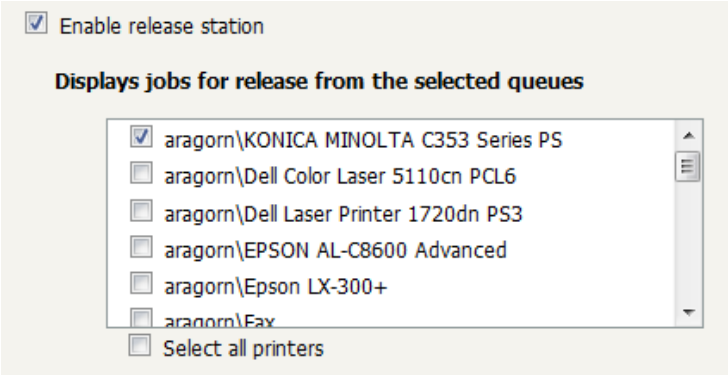
1. In PaperCut, select the “Printers” tab.
2. Select the print queue (i.e. not the ‘device’) for the Konica Minolta device that will be used for testing.
3. Enable the “Hold/release queue” option.



4. Press OK/Apply to save the changes. All printing to this queue will now be held until released by a user.

Make sure the copier is enabled as a “Print Release Station”.

1. In PaperCut, select the “Devices” tab.
2. Select the Konica Minolta device.
3. Under “Device function” to make sure “Enable print release” is ticked. If you have followed the installation steps from the previous chapter, this function will already be enabled.
4. Select the print queue that was enabled for hold/release above. The Konica Minolta device will allow jobs on the selected queues to be released.

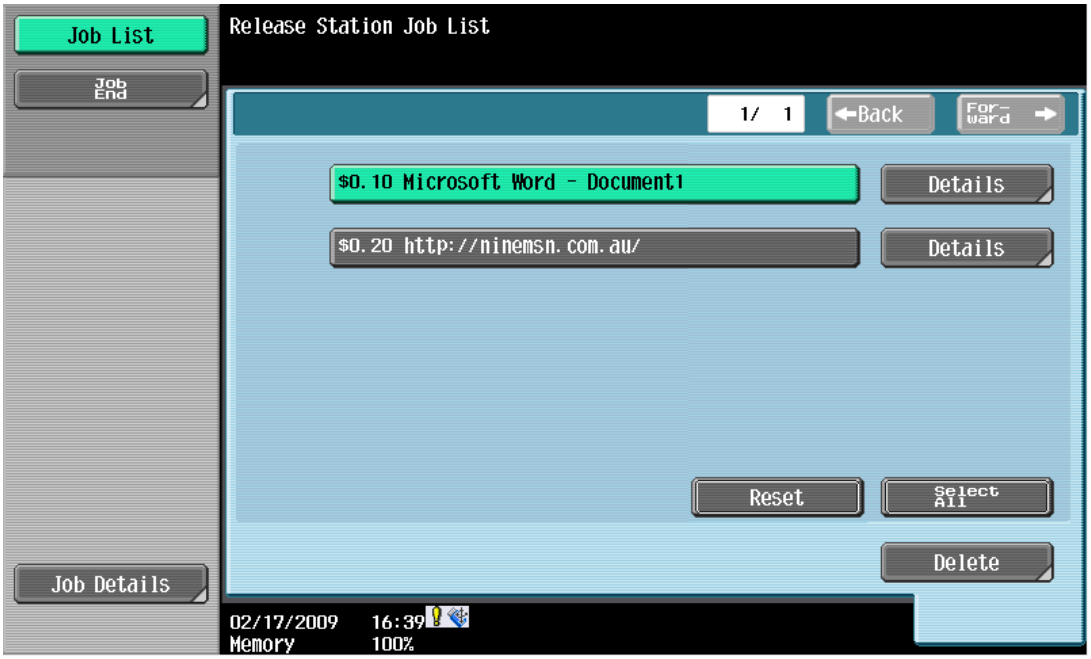


5. Press “OK” to save.
6. Login to a computer workstation as ‘testusersimple’.
7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
8. Confirm that the jobs are held, by checking that the jobs are listed in the “Printers -> Jobs Pending Release” page of the PaperCut administration interface.
9. Confirm that the username is ‘testusersimple’.

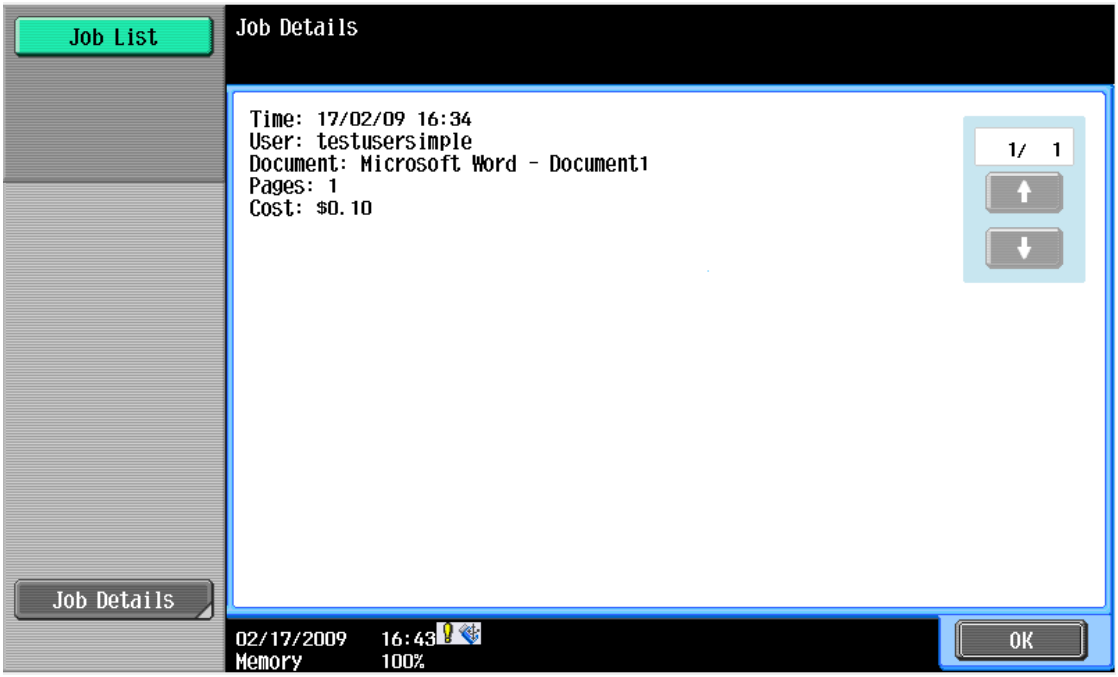
At the device:

1. Log in with the ‘testusersimple’ username and corresponding password as in scenario 1.
2. Note that you can select a shared account at this time since the authentication screen provides access to both the copying and print release functionality. The selected account however only applies to the copying done. Released print jobs will be charged to the account selected when printing.
3. Press the “Release” button on the left of the screen.

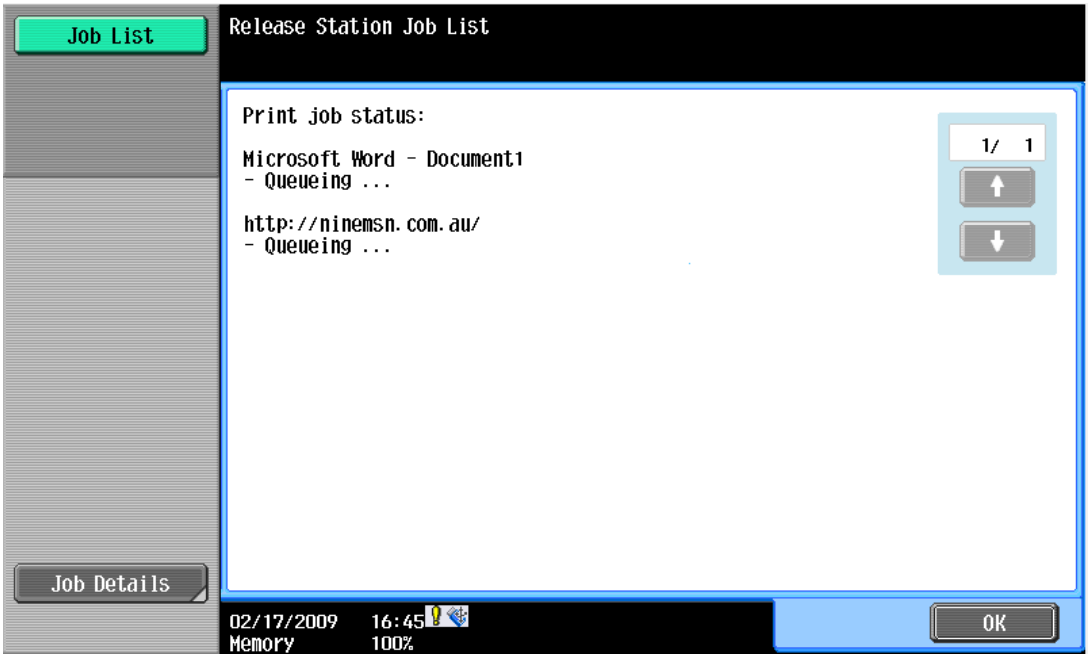
4. A list of print jobs will show. You can highlight and unhighlight individual items by pressing the list item:



5. Press the “Details” button next to a list item to display details about the print job. Go back with “OK”.



6. Now select one or more items and press the “Start” button on the button panel of the device. The print jobs will be queued for printing and a confirmation screen as below will show.



7. Dismiss the confirmation by pressing “OK”. This will take you back to the list of print jobs which may now be empty.

8. To cancel one or more print jobs, highlight the print jobs by pressing the list items and press the “Delete” button on the screen. Confirm with “OK”.

9. Finish releasing or deleting jobs by pressing “Job End” at the top left of the screen.

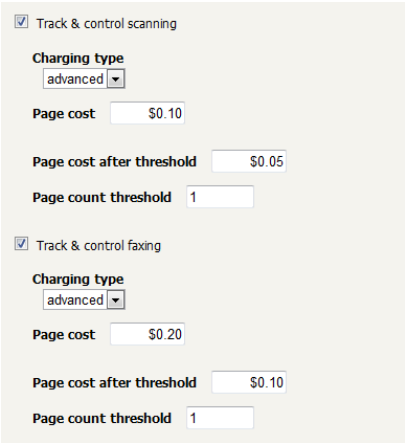
10. To log out, press the “Access” button on the device’s button panel and confirm by pressing “Yes” and “OK”.

3.5 Scenario 4: Scanning and faxing

Konica-Minolta devices can also scan documents and send them by email. If a phone line is attached, they can send faxes. You can enable tracking scanning and faxing. Users can be prevented from scanning or faxing when they are out of credit.

To enable tracking of scans and faxes:

1. In PaperCut, select the “Devices” tab.
2. Select the MFD device.
3. Under “Device function” tick “Track & control scanning” and tick “Track & control faxes”.
4. Select the charging type “advanced” in both cases and set some numbers for page costs and thresholds. The cost after the threshold should be lower than the standard cost as it represents a volume discount. As an example, the screen shot below shows that the first page of a fax is charged at $0.20 and any subsequent page at $0.10.



At the photocopier:

1. Log in using username and password as ‘testusersimple’.
2. The copier will initially show the copy settings screen. Press the “Fax/Scan” button on the device panel and proceed to do some scanning and send some faxes.
3. Once completed scanning and faxing log out by pressing the “Access” button on the device panel and confirm “Yes” on the screen.

In the PaperCut administration interface verify that the scan and fax activities were recorded and the user’s account was deducted. This can be done as follows:

1. Log in to the PaperCut administration interface.
2. Select the device from the “Devices” tab.
3. Select the “Job Log” tab. This will list all recent activity on the copier, including copying, scanning and faxing. The jobs just performed as the test user should be listed. Verify the details of the jobs that were just performed.

Usage Date ▼	User	Charged To	Pages	Cost	Document Name	Attrib
Dec 9, 2009 11:45:23 AM	testusersimple	testusersimple	2	$0.30	[fax]	
Dec 9, 2009 11:44:35 AM	testusersimple	testusersimple	5	$0.30	[scanning]	

4. Click on the user's name in the user column to view the user's account details.
5. Select the "Job log" tab to display all activity for the user.
6. Select the "Transaction History" tab and verify that the cost of the scans and faxes was deducted from the user's account.

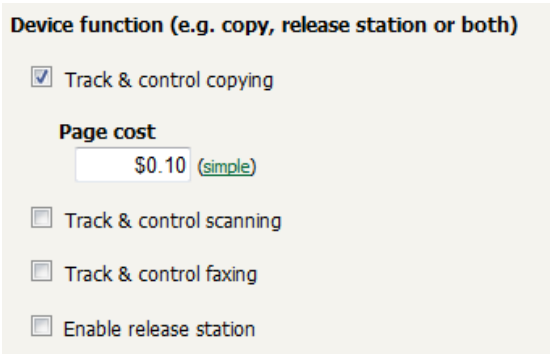
Transaction date ▼	Transacted by	Amount	Balance after
Dec 9, 2009 11:45:23 AM	[system]	-$0.30	$4.40
Dec 9, 2009 11:44:35 AM	[system]	-$0.30	$4.70

4 Configuration

After completing the Installation section and registering the device with PaperCut, it will have been configured with reasonable default settings that are suitable for most environments. This section covers how to change the default settings. All the following settings are available via the device's 'Summary' tab in the PaperCut administration interface.

4.1 Device Function

The device function setting defines which functions will be available on the device and how it will be used. Not all function settings are supported on all devices.



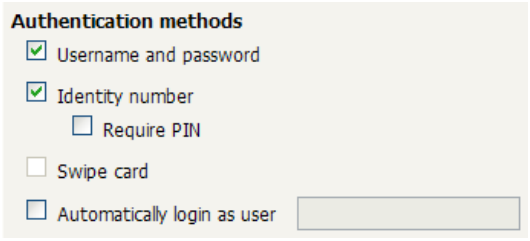
Each device function is discussed in the following table.

Device Function	Description
Track & control copying	The device will track walk-up off-the-glass copying.
Track & control scanning	The device will track scanning such as scan-to-email or scan-to-file.
Track & control faxing	The device will track the sending of faxes.
Enable print release	The device will act as a print release station.

4.2 Authentication Methods

PaperCut supports a number of different ways to authenticate users who walk-up to the devices to perform copying. The default authentication method is username and password authentication.

The available authentication methods can be modified in the 'External Device Settings -> Authentication methods' section.



Authentication methods available for a device

Not all authentication methods are supported on all devices. A grayed-out option indicates that the option is not supported on this device.

Each authentication method is discussed in the following table.

Authentication Method	Description
Username and password	The user may use their domain/network username and password to log into the device.
Identity number	The user may log in with their identity number. Identity numbers are convenient when usernames are long or cumbersome to enter. For example, rather than entering a username like 'john.smith.001', it may be more convenient to enter an employee ID of '1234'. See the PaperCut user manual for information about user identity numbers, including importing identity numbers from an external source.
Identity number -> Require PIN	When a user logs in with their identity number, they must also provide their associated PIN. This provides additional security for identity number logins.
Swipe card	The user may log in by swiping a card (e.g. smart card, RFID and supported by the device). See the PaperCut user manual for information about user card numbers, including importing card numbers from an external source.
Swipe card -> Require PIN	When a user logs in by swiping a card, they must also provide their associated PIN. This provides additional security for swipe card logins.
Automatically login as	Specifies that this device should always automatically log in as the given

user	user. This option overrides all other authentication methods

Description of authentication methods

4.3 Customizing Text and Messages

PaperCut allows some text that appears in the device to be customized. The custom text might include instructions or terminology that is more appropriate for the site. An example of text that is customizable is the “welcome text” that displays before the user logs in to the device.

The text can be customized by editing the device configuration from the PaperCut administration interface. For more details see the Advanced Configuration section.

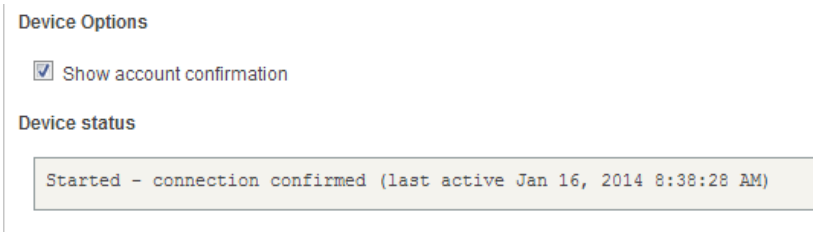
5 Advanced Configuration

5.1 Config Editor

The common configuration options for a device in PaperCut are available on the device's 'Summary' tab, and are discussed in more detail in the Configuration section. This section covers the more advanced or less common configuration options which are available via the 'Advanced Config' tab in the device details screen.

Config name	Description
ext-device.card-self-association.use-secondary-card-number	Select whether user self-association should occupy the primary or secondary card number. It overrides the global setting unless the keyword "GLOBAL" is specified. This is useful when there is a mix of different non-configurable card readers that read different numbers from an ID card. Set to "Y" to use the secondary card number, "N" to use the primary card number. Default: "GLOBAL" to defer to the global configuration option.
ext-device.konica-minolta.login.show-account-search	If set to "Y" replaces the "Account List" button next to the "Account" for account selection field shown during logon to users with account selection enabled with a "Search" button. "Search" allows searching accounts by text, pressing OK at search text entry will display all accounts. This is convenient for users with many potential accounts to charge to, however once enabled this will be enabled for all users including those with short account lists who will have to press OK at search text entry to display the whole list.
ext-device.konica-minolta.locale	Enter the locale (language setting) for display on the device in form xx or xx_XX if different from the server. Examples: "fr" or "pt_PT".

ext-device.konica-minolta.message.welcome.line1 and ext-device.konica-minolta.message.welcome.line2	Specify two lines of text to appear on top of the “Authentication” screen in place of the default message. These can include instructions on which username and password are valid for the device. The value “DEFAULT” in both fields will re-enable the default text.
ext-device.konica-minolta.auth.screen.title	Change this to change the title of the authentication screen.
ext-device.konica-minolta.login.show-account-code	(OpenAPI 3.1+ only) Setting this to “N” will remove the “Account Code” field on the account selection screen. If users are not configured to select accounts by code, this field will not be necessary and removing it reduces confusion.
ext-device.konica-minolta.login.show-user-list	Setting this to “Y” will display a “User List” button next to the “Username” input field on the authentication screen. The “User List” button will display an alphabetical list of all users in the system, allowing for convenient selection of a user name instead of having to type it in. This option is only useful for installations with a small number of users (in the tens of users) as otherwise the “Forward” button will have to be used many times to page through the list.
ext-device.konica-minolta.login.host-based.enabled	(OpenAPI 3.1+ only) Enables support for external host-based authentication (eg TWAIN based scanning, PageScope Web Connection) if set to “Y”. Otherwise external authentication is not allowed (other than logging-on physically on the MFP). Users are required to login using username and password. See section 5.4.

ext-device.konica-minolta.login.host-based-authentication.enabled	(OpenAPI 3.1+ only) Enables secured login for external host-based authentication (if host-based logins are enabled). If set to Y, Users connecting via “PageScope Web Connection”, TWAIN or another external mechanism will need to provide valid credentials. Concurrent use of device externally while someone else is logged on physically is disallowed. Note that on some models enabling this option may interfere with USB printing reliability. If set to N, Users are not required to provide valid credentials to perform TWAIN scanning or login to the device externally. See section 5.4. Default: N
ext-device.konica-minolta.login.confirmation.enabled	Setting this to “N” allows you to bypass the confirmation screen shown after a successful login. Note that this was replaced in by the standard configuration checkbox “Show account confirmation” on the device summary tab. The old setting will be automatically migrated across. 
ext-device.card-no-regex	See chapter 5.3 “Configuring Swipe Card Readers”
ext-device.konica-minolta.restricted.allow-multiple-login	Setting this to “Y” will allow users to log in and charge copy jobs to a restricted account (user account or shared account) if another copy job charged to the same account is still in progress. This may cause cost overruns with users going into negative balance.

ext-device.konica-minolta.card-decoder-hid	Selects the method used to read a user ID from an HID RFID card reader. 0 → the card number field from OmniKey readers is used as the PaperCut user ID. 1→ the entire data on the reader is used as the PaperCut user ID.
ext-device.konica-minolta.card-decoder-force-mode	Overrides card reader auto detection and forces a decode mode, useful where reader detection and consequently decoding of card numbers is unreliable. Currently supports the following values: • DEFAULT – Automatic mode • AU201 – Force decoding of numbers compatible with AU201 card reader • RAW_HEX – Skip decoding and output hexadecimal encoded values sent from the card reader as is, useful for interfacing with custom JavaScript converters. • HID_PROX – Force decoding of numbers compatible with Omnikey Cardman 5125 card reader.
ext-device.konica-minolta.email.personalized-sender	(OpenAPI 3.1+ only) If set to “Y” will pre-populate the email address in the device’s Scan-to-Me function as stored in the user’s details in PaperCut
ext-device.konica-minolta.display-balance	(OpenAPI 3.1+ only) If set to “Y” will display the balance on the device’s screen while using copier functions. Display will not be accurate for users with overdrafts. Unrestricted users will display as “99999999”. Set to “DEFAULT” or “N” to not display balance.
ext-device.konica-minolta.skip-setup	(OpenAPI 3.1+ only) If set to “Y” will skip reconfiguring the device each time a setting is changed in the PaperCut Admin web interface, or the server is restarted. Must be set back to “N” to apply settings. **Warning:** Use with care. This setting is not recommended for most environments - setting this to “Y” Values: Y, N. Default N

ext-device.konica-minolta.escrow-timeout.mins	(OpenAPI 3.1+ only) Period of any one user's inactivity (default: 20 mins) after which the user is assumed to have left the device and finished all copying in case a "log out" has not been reported by the device, e.g. in case of network outages or device firmware defects. The user will then be granted access to his remaining funds in case of escrow and restricted users are allowed to log in again. Contact your reseller or Authorized Solution Center before changing this option. You can find their contact information in your PaperCut Admin interface on the **About** page.
ext-device.konica-minolta.session-timeout.mins	(OpenAPI 3.1+ only) Period of any one user's inactivity (default: 1440 mins = 24 hours) during which jobs started in the user's session can be finished and accounted for in case a "log out" has not been reported by the device due to network outages or device firmware defects. Contact your reseller or Authorized Solution Center before changing this option. You can find their contact information in your PaperCut Admin interface on the **About** page.
ext-device.konica-minolta.compatibility-mode	(OpenAPI 3.1+ only) Modifies job logging and accounting behavior to accommodate scanning and other embedded applications that rely on the authenticated user name in the device. Enabling this option invalidates zero-stop handling and shared accounts. Contact your reseller or Authorized Solution Center before changing this option. You can find their contact information in your PaperCut Admin interface on the **About** page.
ext-device.konica-minolta.login-confirmation-message	(OpenAPI 3.1+ only) Allows for an optional text to be configured and presented as part of the overall login confirmation screen message/instructions when the user logs in to the device.
ext-device.konica-minolta.models-w-optional-username-field	(OpenAPI 4.0+ only) Hides an incorrectly displayed user authentication prompt when printing from USB. Valid values: Comma-separated list of model numbers. **Note**: Model numbers are not case sensitive. For example, if a site has KM c280 and c452 devices, the key should be set to ext-device.konica-minolta.models-w-optional-username-field=c280,c452. **Important:** You must restart the Application Server for the change to take effect.
ext-device.konica-	(OpenAPI 4.0+ only) Allow users an overdraft for a single login

minolta.elastic-balance	session. Enter a positive value for the amount of overdraft allowed. Default: No overdraft is allowed.
ext-device.konica-minolta.limit-device-function.zero-balance	(OpenAPI 4.0+ only) When the user has a zero balance, remove from the device any function that has a cost associated with it and is tracked by PaperCut MF. Values: Y, N. Default N
ext-device.konica-minolta.card-decode-scheme	(OpenAPI 4.0+ only) Sets the card reader scheme. Valid values: • 15.2— Use this value if you have upgraded to PaperCut MF 15.3, use the AU205 (5427) card reader, and the card numbers stored in PaperCut are incorrect. • 16.3—Use this value if you have upgraded to PaperCut MF 17.0, use the AU201 card reader, and the FelicaIDm card numbers stored in PaperCut are incorrect. • DEFAULT—Latest card reader scheme supported.
ext-device.konica-minolta.app-button.title	Configures an optional custom title for the application button label that appears on the application list screen if print release application is installed. For example, instead of using default label of 'Release' for print release application, this can be set to the desired custom value. This affects both the link label displayed on the device and the application name.
ext-device.konica-minolta.app-release.title	Allows customizing of the PaperCut's print release application title without also customizing the link label that appears on the device screen. If there are multiple applications installed on the device such as a third party application together with PaperCut print release application, they may be grouped together on the device in a separate screen. In this scenario the link button on the device panel may need to be customized to something generic, and PaperCut print release app to something specific, in such case use ext-device.konica-minolta.app-release.title to define the title for PaperCut application, whilst using ext-device.konica-minolta.app-button.title to define the name of the group of applications.

ext-device.konica-minolta.keyboard-adaptive	Enables PIN and password controls to use adaptive keyboard type. Adaptive keyboard will use a soft keyboard that is most suitable to the MFP location and provides support for locale specific symbols. Y enables adaptive keyboard, N uses ASCII keyboard Values: Y, N. Default: N Note. Supported on models C652/C552/C452-1st onwards, if embedded integration fails on older models, disable this by setting it to N.
ext-device.konica-minolta.keep-device-settings	Enables some device customizations to be retained after embedded restart and re-installation (on supported models). The customizations include any registered home screen shortcuts and public user function limitations. Values: Y, N. Default N
ext-device.konica-minolta.logout-before-app-registration	Forces user logout from a device when an update to PaperCut is being applied to a device. By default, current users are not forced to logout when updates are applied to a device. Changing this value to Y forces user logout from a device while it is being updated. Values: Y, N. Default: N
ext-device.konica-minolta.force-app-registration	Determines whether to force applications to re-register on the MFP. By default, the application is only re-registered when an important configuration change is detected, such as, a server IP address change, UI related changes, allowed authentication methods on the device, and several others affecting behaviour of the application on the MFP. **Warning:** This setting is for temporary use only—do not leave it permanently enabled. After successful setup, Y will automatically reset back to DEFAULT. Values: Y, N. Default N
ext-device.konica-minolta.openapi.username	Allows OpenAPI username to be set for registering with the target MFP if OpenAPI authentication is configured.

ext-device.konica-minolta.openapi.password	Allows OpenAPI password to be set for registering with the target MFP if OpenAPI authentication is configured.
ext-device.konica-minolta.openapi.sslport	Allows default OpenAPI SSL port to be overridden if non-standard port is used. Default: 50003
ext-device.konica-minolta.login.max-stored-sessions	Defines a maximum number of user logins defined by the combination of the user's name and shared account allowed to be created on MFP before automatically clearing least recently used ones. Default: 29000
ext-device.konica-minolta.login.max-session-age-days	Defines a maximum number of days that a user login as defined by the combination of the user's name and shared account to be not accessed before it's removed. Default: 60 days
ext-device.konica-minolta.period.error	Number of seconds to wait before the Application Server tries to connect to the device again when a set up error occurs while configuring a device or removing device integration. In general, setup errors are error responses received from the device (that is, an OpenAPI call is sent and an OpenAPI response indicating an error is received). Also applies to cases where the device is in fault mode in response to a periodic setup confirmation call. Default: 60 seconds (Range: 1-3600 seconds)
ext-device.konica-minolta.period.fatal	Number of seconds to wait before the Application Server tries to connect to the device again when a FATAL set up error occurs while configuring a device or removing device integration. In general, FATAL setup errors are error responses indicating a broken communication channel while attempting to configure the device (for example, SSL errors, SOAP errors). Other errors considered FATAL: device fault during setup, device with no HDD, Unknown setup error not falling under any other group.

	Default: 300 seconds (Range: 1-3600 seconds)
ext-device.konica-minolta.period.ping	Number of seconds between periodic calls initiated by PaperCut MF to a device, to confirm that it is online. It should take PaperCut MF at most (period.ping) seconds to detect that the device is offline. Default: 300 seconds (Range: 1-3600 seconds)
Additional options for OpenAPI 2.3 devices	
ext-device.konica-minolta.login.show-account	Setting this to “N” will remove the account field from the “Authentication” screen. If charging to accounts is not an option for any user in your system, the account field can be removed for simplicity.
ext-device.konica-minolta.login.show-account-list	Setting this to “N” will remove the “Account List” button next to the account field on the “Authentication” screen. The account list may contain confidential information and should not be visible to all users. Users can still charge to accounts by entering the name or code of an account in the account field.
ext-device.konica-minolta.limit-reference.paper-size and ext-device.konica-minolta.limit-reference.duplex	PaperCut will deny device access to restricted users who do not have enough balance to copy and assign allotments of pages for copying on login. To determine if a user has enough balance to copy and to compute the allotted number of pages on login, a reference copy is required. By default, PaperCut checks if the user has enough balance to copy one single sided Letter (North America) or A4 (worldwide) page. In some situations, it may be desirable to change the reference copy, such as when the device allows smaller page sizes like A5. Default for ext-device. konica-minolta.limit-reference.duplex: N (No) Default for ext-device. konica-minolta.limit-reference.paper-size in North America: Letter Default for ext-device. konica-minolta.limit-reference.paper-size worldwide: A4
ext-device.konica-minolta.paper-size.regular and	For accurate accounting, Konica Minolta devices can be supplied with two sizes of paper, one Letter or A4 (”regular”) and one Ledger or A3 (“large”). Specify the supplied paper sizes here. The “regular” size should be equal to “ext-device.konica-

ext-device.konica-minolta.paper-size.large	minolta.limit-reference.paper-size" above for accurate accounting.
ext-device.konica-minolta.duplex.detection	Optionally switch off duplex detection. Duplex detection is subject to limitations as discussed in chapter 7.10.3 " Duplex Detection". If set to "N" no duplex discount – if defined – will be applied to copies.
ext-device.konica-minolta.restricted.max-pages-per-login	Sets the number of pages users can copy in one login session when charging to a restricted account (user account or shared account).
ext-device.konica-minolta.logout-on-network-reader-swipe	Automatically logs out the first user and logs in the second user, when the second user's card is swiped on the network card reader, whilst the first user's session is active. Values = Y, N. Default = DEFAULT (Y) Set this to 'N' to prevent a second user to be logged in with a card swiped on the network card reader, whilst the first user's session with a card login, is still active. The first user will continue to be logged in with an active session, even if a second user's card is swiped on the network card reader, whilst the first user's session is active.
ext-device.konica-minolta.delete-session.batch-size	Number of sessions that will be cleaned up when the device is inactive. MIN = 1. MAX = 30000. Default = 5 **Note:** 1 session = 1 second (approximately) that the device will be locked and unusable whilst session clean-up is in progress. If this number is very high, the device maybe unusable for an extended period of time.
ext-device.konica-minolta.auth.public-setting	Customize integration with third party applications (EFI Fiery) after device re-initialization. Values = ON_WITH_LOGIN, ON_WITHOUT_LOGIN, RESTRICT. Default = RESTRICT Set this to 'Default (RESTRICT)' to disable integration with third

	party applications after device re-initialization. Set this to 'ON_WITH_LOGIN' to allow integration of third party applications, after device re-initialization, by using the set login method. Set this to ON_WITHOUT_LOGIN' to allow integration of third party applications, after device re-initialization, without the need to login.
ext-device.konica-minolta.avoid-additional-media-info	Customize the sending of information about media types (paper types) to the device. Values = Y, N Default = DEFAULT Setting this to 'Y' will prevent information about media types from being sent to the device. **Note:** This setting will allow bypassing of zero stop for the supported media types. Setting this to 'N' will allow information about media types to be sent to the device. **Note:** If the device does not support certain media types, this setting could result in the device becoming unusable. At the time of registering the device, this value is first set to 'Default' and then based on the media types supported by the device, this value gets automatically re-set to 'Y' or 'N'. If the default setting is overridden and manually re-set to 'Y' or 'N', then after device re-initialization, this value will never be automatically re-set by assessing the media types supported by the device.
ext-device.konica-minolta.user-auth.auto-override	When PaperCut MF is being registered on the device for the first time, and if native device authentication is already enabled and being performed by another application, then the PaperCut MF registration on the device is halted and will continue only after any one of the following actions is taken: • either, this key's default setting is changed from N to Y • or, the existing native device authentication application is manually disabled. Values: Y, N Default: N Setting this to Y will automatically disable the existing authentication application on the device, remove all traces of

	cached authentication data and settings from the device, and continue with PaperCut MF registration on the device. Setting this to N will require the existing authentication application on the device to be manually disabled in order to continue with PaperCut MF registration on the device.
ext-device.konica-minolta.release.show-cost	Toggle the display of the cost of held print jobs on the Print Release screens. Values: Y (show cost), N (hide cost) Default: Y
ext-device.self-association-allowed-card-regex	Customize the regular expression filter to be used to validate card identifiers during card self-association. This is a device-specific config key. • Values: Any valid regular expression, DEFAULT • Default: DEFAULT **Note:** This is applicable only if the **Swipe card** - **Enable self-association with existing user accounts** authentication method is selected. For more information, see 4.2 Authentication Methods and 5.3.1 Methods of handling card identifiers.
ext-device.card-no-regex	Customize the regular expression filter to be used to extract card identifiers for authentication. This is a global and device-specific config key. Device-specific: • Values: Any valid regular expression, GLOBAL (inherited from global settings) • Default: GLOBAL (inherited from global settings) Global: • Values: Any valid regular expression **Note:** This is applicable only if the **Swipe card** authentication method is selected. For more information, see 4.2 Authentication Methods and 5.3.1 Methods of handling card identifiers.
ext-device.card-no-converter	Customize the converters (standard format converters, custom JavaScript converters, or both) to be used to modify card identifiers for authentication.

This is a global and device-specific config key.

Device-specific:

- Values: Any valid converter (standard format converters, custom JavaScript converters, or both), GLOBAL (inherited from global settings)
- Default: GLOBAL (inherited from global settings)

Global:

- Values: Any valid converter (standard format converters, custom JavaScript converters, or both)

Note: This is applicable only if the **Swipe card** authentication method is selected. For more information, see 4.2 Authentication Methods and 5.3.1 Methods of handling card identifiers.

5.2 Setting an explicit PaperCut Server Network Address

The copier connects to the PaperCut server to validate user credentials, display print jobs for release, etc. The device makes inbound network connections to the PaperCut server using a network address of the PaperCut server. By default, PaperCut will use the server's IP address (if the server has multiple IPs (i.e. multi-homed) then PaperCut will select one of them), but on some networks this address may not be publicly accessible from other parts of the network.

If the PaperCut server has a "public" IP address or DNS name then this can be used instead, which allows the copiers to use the "public" network address instead of the IP address that PaperCut detects. To do this:

- Login to PaperCut
- Go to the "Options" tab.
- Select "Config Editor (Advanced)", from the action links on the left.
- Find the "system.network-address" setting.
- Enter the public network address for the PaperCut server.
- Press the "Update" button next to the setting and confirm the setting is updated.

When connecting devices to a PaperCut site server, you can configure the sites' "Network address used by devices":

- Login to PaperCut
- Go to the "Sites" tab.
- Select the site to edit.
- Change the "Network address used by devices".
- Save the site details.

To have either of these changes take effect immediately, restart the PaperCut Application Server service (i.e. on Windows use: Control Panel->Admin Tools->Services).

5.3 Configuring Swipe Card Readers

All keyboard-wedge mode emulating USB card readers are supported. In addition to this, the following card readers are also supported:

- AU-201 (MIFARE/Type-A cards).
- HID Omnikey CardMan 5125 (HID Proximity cards).
- AU-202H (HID iClass cards)
- AU-205H / HID Omnikey 5427CK (HID Proximity/MIFARE/Type-A cards).
- Network card readers (Elatec TWN3 with the TCP Converter/RFIdeas ethernet card readers). These are set-up similarly to the "Fast Release" configuration in PaperCut where the device is associated with the network reader via its IP/port. Both, card reader connected to main MFP and network card reader cannot be used simultaneously.

Important: To use a network card reader, you need to disable the device's inbuilt card reading functionality (even if no card reader is attached) in Service Mode.

Compatible card readers are limited to those supported by Konica Minolta firmware. PaperCut's embedded solutions are designed to support as many card readers as possible and will add new card reader supported as new devices come available at the firmware level. AU-205H Keyboard Wedge Mode is supported.

The AU-202H readers which are HID proximity card readers will work in place of AU201 but extraction of real card numbers is only possible via a custom JavaScript converter.

Some models do not support all of the listed readers. Please confirm the specifics for the model in question with your local Konica Minolta dealer.

5.3.1 Methods of handling card identifiers

By default, PaperCut MF handles each card's unique identifier using the following pre-configured method:

- Cards whose identifiers consist of a number followed by special character and a checksum, are modified to include only the number (the special character and everything after it is ignored). This extracted, shortened identifier is used to identify the card and the corresponding user within PaperCut MF. For example, a card with the unique identifier 5235092385=8 is modified to 5235092385.

You can also tweak the way PaperCut MF handles each card's identifier by using any of the following methods:

- Using utility or configuration tools directly on the card reader's hardware.
- Using third party applications to decrypt card identifiers. For more information, contact your reseller or Authorized Solution Center.
- Using the following methods within PaperCut MF:
    - Regular expression filters
    - Converters (standard format converters and custom JavaScript converters)

    Note: If you use both an expression *and* a converter, then the card's identifier is handled first by the expression and then further by the converter

Verify the results of the expressions, convertors, or both applied using the PaperCut MF Admin web interface's **Application Log**.

5.3.1.1 Regular expression filters

To extract card identifiers using regular expression filters, use the config keys **ext-device.self-association-allowed-card-regex** and **ext-device.card-no-regex**. For more information, see 5.1 Config Editor.

Some regular expression filters include:

Expression	Description	Example
(.{10})	Extract the first 10 characters	AST%123456789 is modified to AST%123456
(\d{5})	Extract the first 5 numbers	AST%123456789 is modified to 12345
\d*=(\d*)=\d*	Extract only the numbers between the 2 special characters	123453=292929=1221 is modified to 1234532929291221

For more information, see www.regular-expressions.info.

5.3.1.2 Standard format converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see 5.1 Config Editor.

Some examples of standard format converters are:

Converter	Description	Example
hex2dec	Convert a hexadecimal (base 16) encoded card identifier to the decimal format. **Note:** Hexadecimal numbers usually contain 0-9 and A-F.	946EBD28 is modified to 2490285352
dec2hex	Convert a decimal encoded card identifier to the hexadecimal format.	2490285352 is modified to 946EBD28
ascii-enc	Unpack an ASCII encoded card identifier to its encoded ASCII number.	3934364542443238 is modified to its ASCII code 946EBD28.
ascii-enc|hex2dec	First unpack an ASCII encoded card identifier to its encoded ASCII number. Then convert it to the decimal format.	

Note: Use a delimiting pipe (|) to chain or pipeline converters.

5.3.1.3 Custom JavaScript converters

To use a custom JavaScript converter:

1. Create a JavaScript file. For example:
   [install-path]/server/custom/card.js
2. Define a single JavaScript function in this file called **convert**. It must accept and return a single string. For example:
   ```
   function convert(cardNumber) {
     return cardNumber.substring(3,10).toLowerCase();
   }
   ```
3. Include a converter in the form: **javascript:custom/card.js**
4. Optionally, include a JavaScript script in the pipeline. For example:
   ascii-enc|hex2dec|javascript:custom/card.js
5. Verify the JavaScript converter from the following log:
   [install-path]/server/log/server.log
6. Use the config key **ext-device.card-no-converter** to modify card identifiers using custom JavaScript converters. For more information, see 5.1 Config Editor.

5.4 Host-based authentication

Host-based authentication refers to any external login to the MFP (originating from another host).

This can be a desktop application such as a TWAIN driver or a web based application such as “PageScope Web connection”.

Desktop based scanning applications using TWAIN drivers to communicate with the device require “host-based authentication” to be enabled.

In this case a device-controlled driver or software pops up a dialog to collect any credentials and to have the user confirm their action.

PaperCut has limited support for applications requiring host-based authentication. This support can be enabled via the advanced configuration option “ext-device.konica-minolta.login.host-based” (see section 5.1).

Applications requesting host-based authentication will cause a popup to display on the desktop showing username/password fields and an input field labeled “account” and “OK” and “Cancel” buttons. The account field is a dummy field, owing to limitations of the device, and any input will be discarded. The user is to use their username and password to authenticate and go ahead with an action, such as scanning.

NOTE: It is possible to allow use of anonymous logins for host-based sessions (see section 5.1).

NOTE: No tracking or charging of jobs requiring host-based authentication will occur by default. Should a user be logged in on the device’s panel at the same time the job is authenticated at the desktop, the job will be charged to the user logged in at the panel.

6 Uninstalling

In order to remove PaperCut authentication and print release functionality from the device:

- Make sure the device is switched on, connected and the status on the “Device Details” screen shows “connection confirmed”.
- Delete the device in PaperCut by clicking “Delete Printer” from the “Device Details” screen. Warning: This will also delete your settings for this device such as page cost settings.
- The device screen will go blank and show a message “Now remote operating.” Wait until it returns back to normal after 10-15 seconds, showing the standard copy settings screen.

In order to reactivate PaperCut functionality on the device, recommence installation as per the installation chapter of this document.

7 Known Limitations and Security

The Konica Minolta OpenAPI environment has a number of limitations that have an impact on functionality and security.

7.1 Screen Workflow

Although the multi-screen workflow introduced in newer OpenAPI 3.1+ devices has improved, it is still not ideal due to limitations in screen layout and a fixed number of controls. Moving forward PaperCut will start leveraging the device’s embedded web browser for screen design, bringing the solution up to a level seen on other makes. Although the embedded web browser is an option today, the cost of additional hardware and firmware makes it currently prohibitive. We hope this will change in future versions. Areas of concern in the current release are:

- The default screen workflow used to allow users to self-associate their cards with their account is a little counter intuitive (warning dialogs used to convey workflow).
- Users can not set/reset card PINs at the device.
- It’s not possible to adapt screen layout based on user rights (e.g. hide the account PIN/Code field if the user does not have rights to use this field).
- Selecting account takes too many key presses.

7.2 Combining Auto-color and Duplex

A duplex copy job with the “auto color” color setting that has mixed color and black-and-white pages will not differentiate between the color mode of the front and back side of a sheet. The color mode of both pages will be recorded as that of the front side.

7.3 Copy restrictions on restricted accounts

Users are prevented from logging in with a restricted account (user account or shared account) if another copy job charged to the same account is still in progress. Copy jobs in progress can be viewed using the “Job List” button on the device screen. Once the previous copy job has finished, users can log in again and charge to the restricted account. This behavior can be overridden using a configuration key, please see chapter 5.1.

7.4 PageScope Box Operator PC software

The PageScope Box Operator PC software is not designed to work with an MFP connected to an OpenAPI authentication application (like PaperCut). This is a limitation of the MFP and Box Operator software.

Users still have access to the Box Operator functionality via the devices web browser interface. It is recommended that users use this web interface instead of the PC software.

7.5 Job logging in case of network outages or firmware defects

PaperCut logs any user's jobs after the user logs out and the last job started during the session finishes. In case of network outages or device firmware defects, the log out may not have been reported to PaperCut by the device. PaperCut employs a number of timeout mechanisms to ensure jobs will still get logged eventually.

- After a delay of 1 hour (configurable, see section 5.1) of any user's inactivity, the user is assumed to have logged out and their jobs will be logged. Their funds, if escrowed, will also be made available and – in case of restricted users – logging in is allowed again.
    - Tracking log outs with early firmware releases of the A4 bizhub C35 model (mid-2011) has been shown to be more challenging than with A3 models. The escrow timeout therefore defaults to 10 minutes on those devices.
- After this delay of one hour, jobs being reported as finished by the device will still be logged by PaperCut, with a delay of 5 minutes (configurable, see section 5.1). An example for a job being started during a session and not completing before one hour later may be a job that has been paused due to paper outage.
- Jobs reported after more than 24 hours of one user's inactivity (configurable, see section 5.1) will not be logged or charged to any user.

7.6 Account Selection and Print Release

The authentication process may present an option to select a shared account and – if presented – will enforce that one account be selected. Copies produced will be charged to this shared account, however print jobs released will remain unaffected by this choice and will be charged to the account selected when sending the print job.

7.7 Interface

The Konica Minolta interface options are limited and the PaperCut development team is aware of a number of issues:

- Limitations on color, design and formatting
- Lack of access to features such as adding comments and invoicing options to jobs
- Limits on the length of print job names displayed

7.8 Bypassing the System

It is important that the administrators take care to prevent users from bypassing the system and directly accessing the copier. Likewise, it is also important that administrators know how to bypass/disable the system if direct copier access is required – say to change advanced system settings. Administrations should take the following precautions:

The copier's administrator password should be changed and always kept secure.

7.9 User Box operation

The user box is an MFP feature that provides a document management area on the MFP hard disk. There are public, group and personal user boxes each targeting a particular user scope. The following applies to personal user boxes only.

On MFP models where personal user box is available, PaperCut integration allows limited access to personal user boxes.

If shared accounts are in use by any user logging into the MFP, personal user boxes are accessible only as a combination of the user and the selected shared account. Where user always logs in using a single account, eg. built-in personal account the limitation does not apply.

This means that user logging on to the MFP will see a different personal user box along with its content if they use a different shared account to login.

Thus, a user can have access to multiple user boxes via the virtue of access to their shared accounts.

An MFP stores a maximum of 30000 user logins in its memory, therefore any personal user boxes created as part of logins are automatically removed under the following conditions:

- The number of logins created on a single device exceeds default configured limit
- The login (user/account combination) was not accessed within a configurable period of time
- MFP is removed from PaperCut

Refer to "login.max-stored-sessions" and "login.max-session-age-days" in the Config Editor: 5.1

7.10 Additional Limitations for OpenAPI 2.3 devices

Note: These limitations are not present in OpenAPI 3.1+ devices.

7.10.1 Zero Stop when Copying

In an ideal implementation, PaperCut would be able to control exactly how many pages a user can copy and always prevent the user from overdrawing their account. On Konica Minolta devices, users are assigned an allotment of black & white and a second allotment of color copies according to their account balance and will stay within their credit balance if either number of pages is copied. If both the allotted number of black & white and color pages is copied, the total cost will exceed the available credit and the balance will go into the negative.

In addition, large (A3 or Ledger size) copies are counted as two regular (A4 or Letter) copies for the purpose of this limitation, irrespective of the actual cost settings in PaperCut. If the cost for a large (A3/Ledger) size page is set higher than twice the cost of a regular (A4/Letter) sized page, the available credit can be exceeded by producing large copies only.

7.10.2 Zero Stop when Scanning or Faxing

Konica machines currently do not keep users from performing faxing and scanning beyond their credit limits while logged in, possibly incurring an overdraft on their account. After logging out, users *are* prevented from logging in again while they are out of credit.

7.10.3 Duplex Detection

Users can choose to produce duplex copies (both the front and back side of a sheet are being printed on) by choosing the appropriate option on the copier options screen at copy time. Between logging into the copier and logging out after copying, this option can be turned on and off, producing both duplex and simplex copies. If any copying done between log in and log out includes duplex copies, all copying done between log in and log out will be recorded as duplex in PaperCut job history and the duplex discount – if any – will be applied to all copies produced.

PaperCut Software is working with Konica Minolta to address these issues.

8 FAQ & Troubleshooting

The device screen is showing “Connecting to server …” for an extended period

This message should not appear for more than a few seconds. If this message does not go away (or if it is followed by an error message rather than the normal behavior) then this indicates a problem.

1. Is the device’s network connection functional?
2. Is there a useful error message displayed in the PaperCut admin interface at "Devices -> [device] -> Device status" (gray box)?
3. Try switching off the device for 5 seconds and switching it on again. This may resolve some network connectivity issues.
4. Can the device connect to the PaperCut server on port 9192? You may need to check routers and firewalls, including the Windows software firewall. A good way to test this is to telnet to the server’s IP address on port 9192 (`telnet 1.2.3.4 9192`).
5. Does the device have the latest firmware installed? Connection problems may occur with older firmware versions on some devices.
6. What is the IP address of the primary server? When starting the application server service, e.g. after a reboot or, in Windows, through Control Panel > Administrative Tools > Services > PaperCut Application Server, you will find a line like this in the log file [app-path]/server/logs/server.log:

   ```
   # System details: max memory: 493.1 MB, processors: 2, free space: 119,516.8
   MB, hostname: aragorn, IP addresses: [192.168.1.23,
   fe80:0:0:0:d168:5b94:721c:19b3%10], runtime: 1.6.0_11-b03, time-zone:
   Australia/Sydney, locale: en_AU, encoding: windows-1252
   ```

   The first IP address in the list of "IP addresses: [...]" will be the one that the Konica Minolta device uses to contact the PaperCut server. If you want it to use another address, e.g. if you have multiple interfaces, please change the option "`system.network-address`" in the global config editor, which you will find in the administrator web interface on the “Options” tab, under “Actions” on the left (not to be confused with the device-level config editor on the “Devices” tab).

After restarting the MFP authentication/connectivity to PaperCut application server stops.

This problem may occur even if embedded was running successfully before the restart of the device. Repeating the embedded setup rectifies the problem temporarily until the reboot.

This may occur on some devices if SSDP network protocol is disabled. Even if not used it has to be enabled for the device to support integration with external authentication servers reliably.

The device screen is showing an error message "You copy job has reached its maximum color/black & white allowance" although no user is currently accessing the device

This message appears when a user starts a copy job, walks away and at some point the copy job reaches its maximum allowance. The user that started the copy job or an administrator will have to log in to delete the job.

I am seeing an error in the Device summary page that states "Error: login: error=12, message=no permission"

This message usually indicates that the credentials you've used to connect to the device are wrong. These credentials will be the same as the username and password you enter when logging into the admin UI of the device.

Setup of the Device fails, or subsequently shows an error "Device registered a fault or a component reached end of life"

Device cannot be managed and fails to register with the PaperCut App Server. Sometimes this issue stems from faults with the device or its attachments (for example a faulty feeder or filter).

As an example, this was seen with ozone filters reaching end of life status, or waste basket errors on the device.

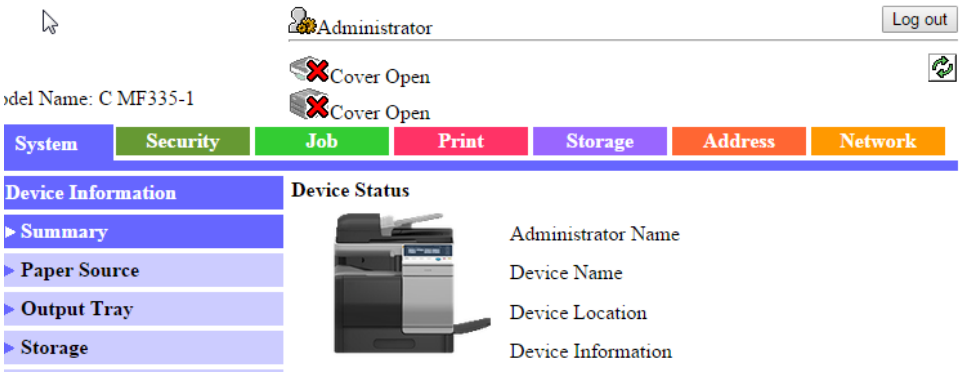
In some cases errors may not show up on the device itself, but normally the MFP returns an error in the PaperCut debug logs:

```
login: error=9, message=Error
```

```
login: error=9, message=Fatal
```

For example: `"2015-03-09 06:59:37,088 ERROR KMExtDevice:346 - login: error=9, message=Error [dev\konica552_workroom]"`

Check if you can login in to the PageScope web connection console, and see if the copier icon shows up with an exclamation mark or a tool next to it with a flashing message/icon:



Ensure that the device error is rectified, and then try embedding the device with PaperCut again.

When using scan to me (email) feature both from and to addresses are set to the user email address.

MFD allows the email address to be set for the machine under administrator settings, however when used together with the authentication application and personal sender is enabled (ext-

device.konica-minolta.email.personalized-sender) the MFD automatically uses this address for both to and from fields in any emails.

If personal sender value is not set, the configured machine email address takes effect and is used as from field but scan to me function is not enabled by the device.

This is a known limitation of the OpenAPI platform.

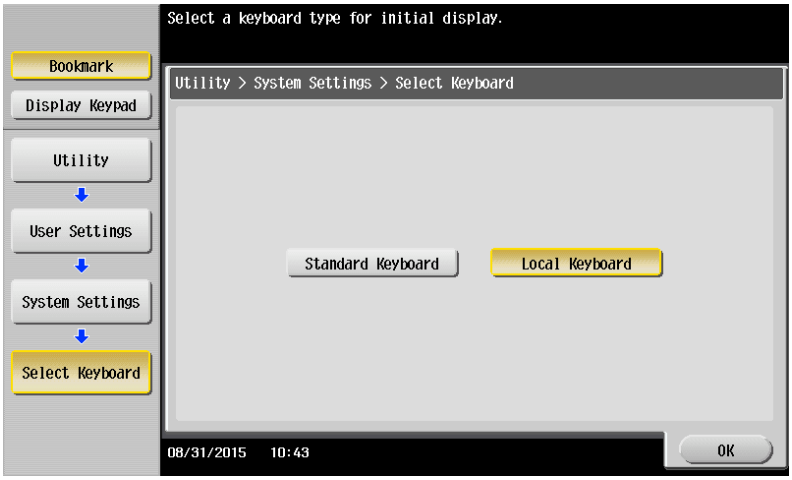
Can I disable the logout confirmation?

The logout confirmation screen is controlled by the copier and can be configured via Utility -> Administrator Settings -> User Authentication/Account Track -> User/Account Common Setting -> Logout Confirmation Screen Display Setting.

Why is the on screen keyboard missing some characters, e.g. the "@" symbol?

The locale and / or language of the keyboard and copier can change the selection of characters available on the on screen keyboard. You may need to select another language and / or locale to obtain characters commonly used in your organisation.

To use locale specific symbols the keyboard type may need to be set to "Local Keyboard" in the panel utility menu. This is set under Utility > User Settings > System Settings > Select Keyboard.



Why do I see an authentication prompt when logged in and printing from USB?

Printing from USB on some MFPs may result in an authentication prompt being displayed when the job is started.

Dismissing the prompt by just acknowledging it and hitting ok without entering any data should allow the job to proceed.

This happens under the following conditions:

- The MFP is configured for use with a card reader **and**
- Any of the following is true:
  - Older version of PaperCut is used.
  - MFP is older than 4th generation
  - Device Type in PaperCut is earlier than OpenAPI 4.x is.
  - Firmware on the MFP is not up-to-date

Why is a user's name displayed with a number in parenthesis appended to it?

When you start a login session on the MFP, a username is assigned to the session to identify the current user of the MFP, which is normally the username.

Sometimes this username is altered to be "user (2)", "user (3)" and so on for subsequent logins by the same user.

This occurs under the following conditions:

- The user has logged on previously to this MFP and performed a job.
- The job did not complete prior to the user logging out (for example, out of paper).
- The user has logged in to the MFP again using another shared account.

If there are incomplete jobs from a previous session, the MFP will not logout from the previous session. The number appended to the username is required to ensure that the user balance and account tracking is done correctly by the MFP.

This means that subsequent logins and any jobs performed with a different account, will track against that account and adhere to its credit limit.

However, the modified username might cause incompatibility with SSO functionality and affect other applications on devices that rely on a consistent username.

If consistent usernames are required, enable compatibility mode using `ext-device.konica-minolta.compatibility-mode`.

Note that enabling compatibility mode limits the accuracy of account quotas and job tracking when sessions are left active by users on the device.

Why is the 'Release' button now called 'APP' on some devices since upgrading to PaperCut 15.3?

The "Release" button has been renamed to "APP", by default, as per Konica Minolta Certification recommendation. You can configure this button to display 'Release' instead by selecting Devices -> [Select Device] -> Advanced Config; then changing 'ext-device.konica-minolta.app-button.title' to 'Release'.

9 Appendix A: Setup and operation on older OpenAPI 2.3 models

9.1 OpenAPI Setup (Older Models)

- Make sure you are logged on as administrator onto the device's web interface (called "Page Scope Web Connection") under http:// <ip-address-of-device>/.
- If the administrator's password hasn't yet been changed from its default value, click the "Security" tab, click "Administrator Password Setting", enter a new password twice and click OK. Make note of this password.
- Now, on the "Security" tab, click "SSL/TLS Setting". If an SSL certificate is shown at this point, skip the following steps:
    - Click "Setting", select "Create a self-signed Certificate" and click "OK".
    - Fill in the fields with some values about your organization. The values have no functional significance.
    - For the Validity Period the maximum number of days offered is recommended (usually 3650 = 10 years).
    - "Encryption Strength" and "Mode using SSL/TLS" can be left to the default values.
    - Click OK. The certificate will be generated and your web browser will re-logon to the web server under "https" mode. You may have to confirm an "invalid certificate" in your browser.
- Again on the "Security" tab under "SSL/TLS Setting", click "Action for Invalid Certificate". If "Continue" is not already selected in the drop-down list, select it and click "OK".
- On the "Network" tab click "OpenAPI Setting". Check "Use SSL/TLS" and set the SSL port number to "50003". Click "OK".
- Again on the "Network" tab, click "TCP Socket Setting". Check "Use SSL/TLS". (The port number is not important.) Click "OK". You may be asked to reboot your device.
- Click "Logout" to log out, switch the device off for 5 seconds and switch it on again.

9.2 Authentication and Account Selection on OpenAPI 2.3 Devices

Due to limitations in devices with OpenAPI 2.3 or a later version less than OpenAPI 3.1 authentication and account selection are reduced to a single step, one screen operation.

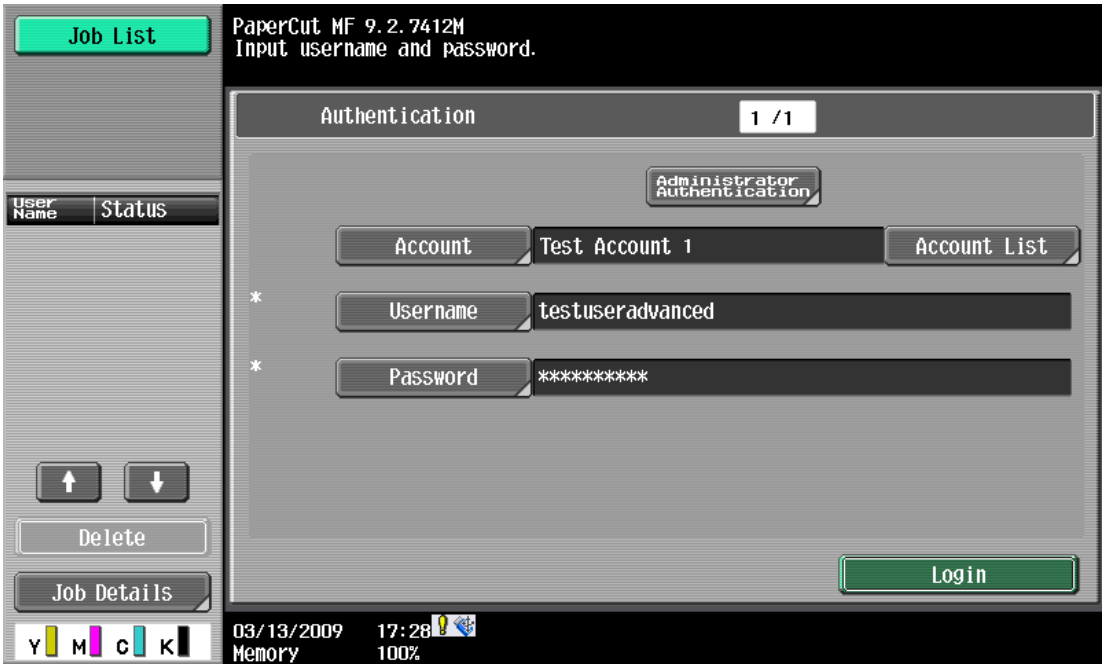
System administrators are encouraged to read the following information, familiarize themselves with the scenarios and educate their users as to the correct operation of account selection.

9.2.1 Authentication with Username and Password or ID

A user wanting to charge the copying to a shared account will have to choose the shared account at the authentication screen, i.e. at the same time as e.g. entering a username and password or an ID number.

- Users having jobs automatically charged to their personal account can leave the account field empty.
- Users having the choice of charging to either their personal account or a shared account will have to select the item "My Personal Account" from the account list, or, if the account is list is not available, enter the account code '0' into the account field.

- For users that can only charge to shared accounts, not to their personal account, the item “My Personal Account” will still show at the start of the account list, however they will be notified after pressing “Login” that this choice is not available to them.



9.2.2 Card-based Authentication

For swipe card authentication, account selection will have to be made at the login screen *before* swiping the card.

As above, users with an option to charge to their personal or a shared account are obliged to make an account choice and when failing to do so will be informed after swiping the card.

