

PaperCut Konica Minolta Embedded Manual

Contents

1	Overview	3
1.1	Consistency:	3
1.2	Integration:.....	3
1.3	Rate of development:.....	3
1.4	Vendor Neutral:.....	3
1.5	Security:.....	4
2	Installation	4
2.1	Konica Minolta Device Compatibility	4
2.2	Requirements	5
2.3	Setup Procedure.....	5
2.3.1	Configure OpenAPI Settings.....	5
2.3.2	Enabling Unauthenticated Printing.....	6
2.3.3	PaperCut Settings.....	7
3	Post-install testing	8
3.1	Test Preparation	8
3.2	Scenario 1: Standard copying.....	9
3.3	Scenario 2: Copying with account selection	12
3.4	Scenario 3: Print release	14
3.5	Scenario 4: Scanning and faxing.....	17
4	Configuration	20
4.1	Device Function	20
4.2	Authentication Methods	20
4.3	Customizing Text and Messages	21
5	Advanced Configuration	21
5.1	Config Editor.....	21
5.2	Additional options for OpenAPI 2.3 devices	22
5.3	Setting an explicit PaperCut Server Network Address.....	23
5.4	Configuring Swipe Card Readers	24
5.5	Card Self-Association.....	25

6	Uninstalling	25
7	Known Limitations and Security	25
7.1	Screen Workflow	25
7.2	Copy restrictions on restricted accounts	26
7.3	Bypassing the System	26
7.4	Account Selection and Print Release	26
7.5	Interface	26
7.6	USB printing and scanning	26
7.7	Additional Limitations for OpenAPI 2.3 devices	27
7.7.1	Zero Stop when Copying	27
7.7.2	Zero Stop when Scanning or Faxing	27
7.7.3	Duplex Detection	27
8	FAQ & Troubleshooting	28
	Appendix A: Setup and operation on older OpenAPI 2.3 models	29
	OpenAPI Setup (Older Models).....	29
	Authentication and Account Selection on OpenAPI 2.3 Devices.....	29
	Authentication with Username and Password or ID	29
	Card-based Authentication	30

1 Overview

This manual provides an overview of the installation, configuration and operation of PaperCut's embedded software MFD (Multi-Function Device) solutions. Today's MFDs are smarter – they have touch screens and offer the ability to run applications directly on the device. The goal of PaperCut Software's embedded MFD solution is to leverage these smart devices and to provide walk-up copier users with the same set of rich application features provided in the print control area. These include:

- Secure access to device functions
- End user authentication including integration with single sign-on environments
- Monitoring and control of photocopying, scanning and faxing (quotas, charging, allocation and logging)
- Allocation of copying, scanning and faxing to accounts/departments/cost-centers/projects
- Release jobs from a hold/release queue (Secure & Find Me Printing)
- Group based access control: Limit access to color copying or to the device as a whole to selected user groups
- Self-associate swipe cards with domain user accounts directly at the device

Highlights of the embedded solution include:

1.1 Consistency:

The embedded solutions are developed in-house by the PaperCut Software development team. This ensures that the copier interface is consistent with the workstation print interface, meaning users only have to learn one system.

1.2 Integration:

PaperCut is a single integrated solution where print, internet and copier control are all managed in the one system. Users have a single account and administrators have the same level of reporting and administration for all services. The embedded solution interacts with the PaperCut server using a Service Oriented Architecture (SOA) and web services based protocols.

1.3 Rate of development:

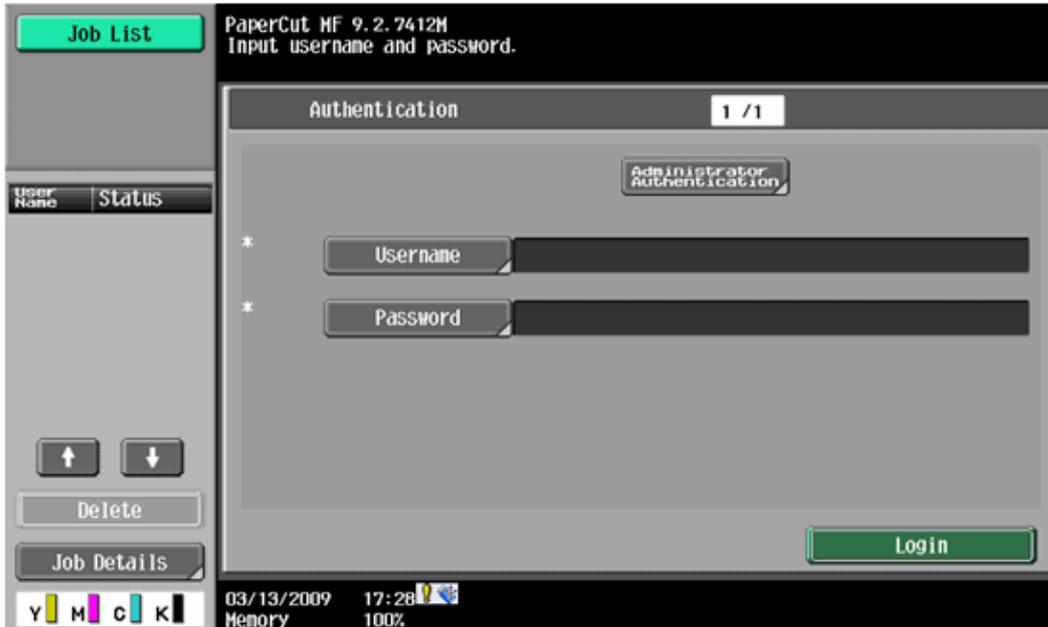
PaperCut is developed under a release-often policy where new features are made available to users as soon as they are complete. Unlike hardware based solutions, new versions can be delivered to users regularly as software updates.

1.4 Vendor Neutral:

PaperCut remains true to its vendor neutral stance. All embedded solutions are equal and support all server OS's including Windows, Linux and Mac.

1.5 Security:

A large percentage of PaperCut’s user base is in Education environments where security is important. All embedded solutions are developed with security in mind. Where security objectives can’t be satisfied, any deficiencies are fully disclosed.



The Konica Minolta onboard/embedded application login screen example

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 Konica Minolta Device Compatibility

PaperCut supports any multi-function Konica Minolta device with “OpenAPI” functionality and a hard drive installed. PaperCut requires OpenAPI version 2.3.1 or higher with version 3.1+ recommended.

Devices with OpenAPI 3.1 or later provide additional comfort during the log and account selection process, allow users to self-associate a swipe card with their existing account and provide more precise accounting and zero-stop while using the copier functions. Please see chapter 7.7 for a details of the limitation of OpenAPI 2.3 devices.

Please note many older devices can have their firmware upgraded to support version 3.1. Please contact Konica Minolta to inquire about firmware upgrade availability for your model.

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>/`. Tip: The default administrator's password usually is "12345678".
- 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.
- If a certificate is shown in the "Device Certificate List", skip the following steps:
 - 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". Your web browser will re-logout to the web server under "https" mode. You may have to confirm an "invalid certificate" in your browser.
- Again 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.
- As a last step, 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.
- For security reasons it is recommended also change the device’s default administrator web access password.

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. 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 IP address and device administrator password are entered as 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.

In addition, a corresponding device option has to be set on the device. On 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 is “12345678”.)
- Select “User Authentication/Account Track”.
- Select “Print without Authentication”.
- Select “Allow”.
- Select “OK”.

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 "Konica Minolta (OpenAPI 2.3+)" or "Konica Minolta (OpenAPI 3.1+)" depending on the version of OpenAPI supported by your device. If unsure, try version 3.1+ first.

Create Device
Allows for the creation of an external device, like a photocopier terminal. Supported hardware is required.

Device name (e.g. Staff room copier, Library cash loader)
Library Copier

Hostname / IP
192.168.1.21

Location/Department (Optional)

Type
Konica Minolta (OpenAPI 3.1+) ▼

- Al Copicode-IP
- Gestetner (ESA)
- HP (Chai SOE DSE)
- Al Konica Minolta (OpenAPI 2.3+)
- Konica Minolta (OpenAPI 3.1+)**
- Lanier (ESA)
- Lexmark MFD (LeS)
- Lexmark Printer (LeS)
- Lexmark Touchscreen Printer (LeS)
- Nashuatec (ESA)
- Ricoh (ESA)
- Savin (ESA)
- Sharp OSA
- Toshiba
- VCC Cash Acceptor
- VCC Controller (Standard)
- VCC Controller (Touchscreen)
- Al Xerox (Network accounting / JBA)

device is created.

OK Cancel

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 release station”.
Enabling both copy and print release station 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 ...”. Please click “Refresh” again a few times until the status field shows “Started - connection confirmed (last inbound none, no panel user, active sessions: 0)”.

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.

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”.

Account Details
To set the user's balance enter the value here. To adjust the amount (like adding 5 credits), select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance
\$5.00 (adjust)

Restricted

Overdraft
Use default overdraft (\$0.00)

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

Account Selection
Account selection can be used to allow the user to select what account is charged, or even to confirm print jobs before they are sent to the printer. These options require running the user client tool on workstations.

Print account selection
Automatically charge to personal account

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.

Account Selection
Account selection can be used to allow the user to select what account is charged, or even to confirm print jobs before they are sent to the printer. These options require running the user client tool on workstations.

Print account selection
Show the standard account selection popup

Information to show in popup

- Allow user to charge to their personal account
- Allow user to select shared accounts (from list)
- Allow user to select shared accounts (using PIN/code)

Warning: This setting requires this user to run the client software at all times.

4. Press the “OK” button to save.

3.2 Scenario 1: Standard copying

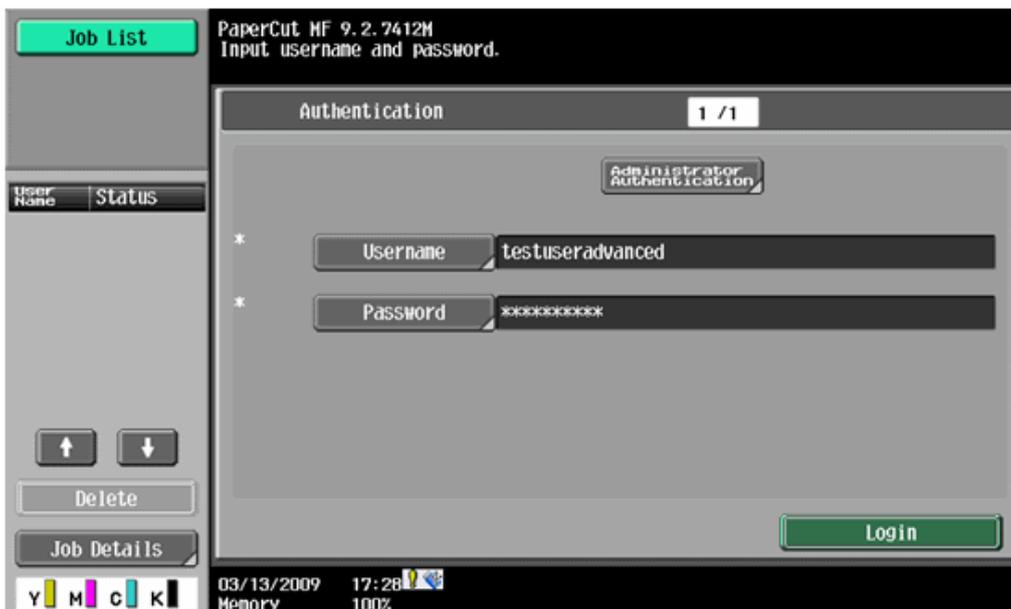
Standard copying involves monitoring/charging printing to a user’s personal account. This is the most commonly used for student printing or basic staff monitoring. Users can also be configured for unrestricted printing, which is commonly used for staff/employee use.

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”.



- The screen will now show a login confirmation:



- At this point the copier will be enabled for usage.
- 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.
- 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.



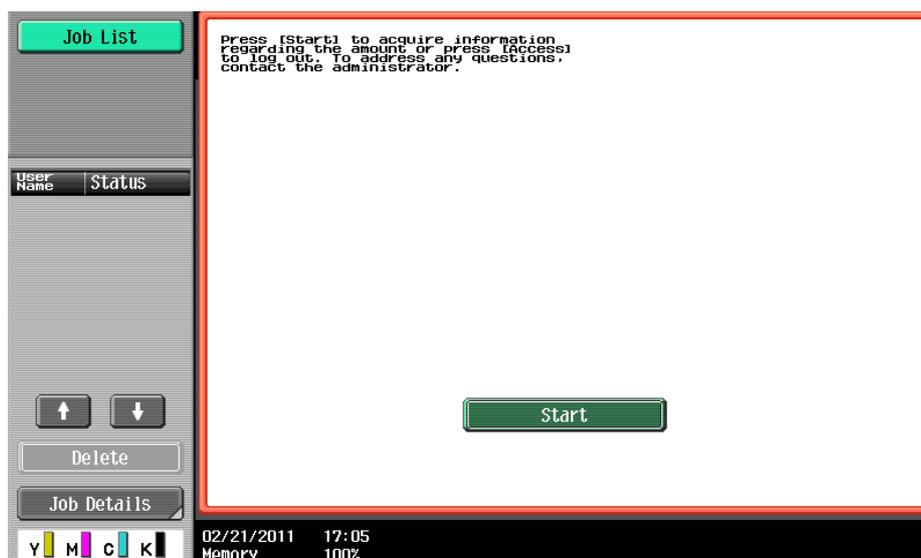
Back in the PaperCut application verify that the copier activity was recorded and the user’s account deducted.

- 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

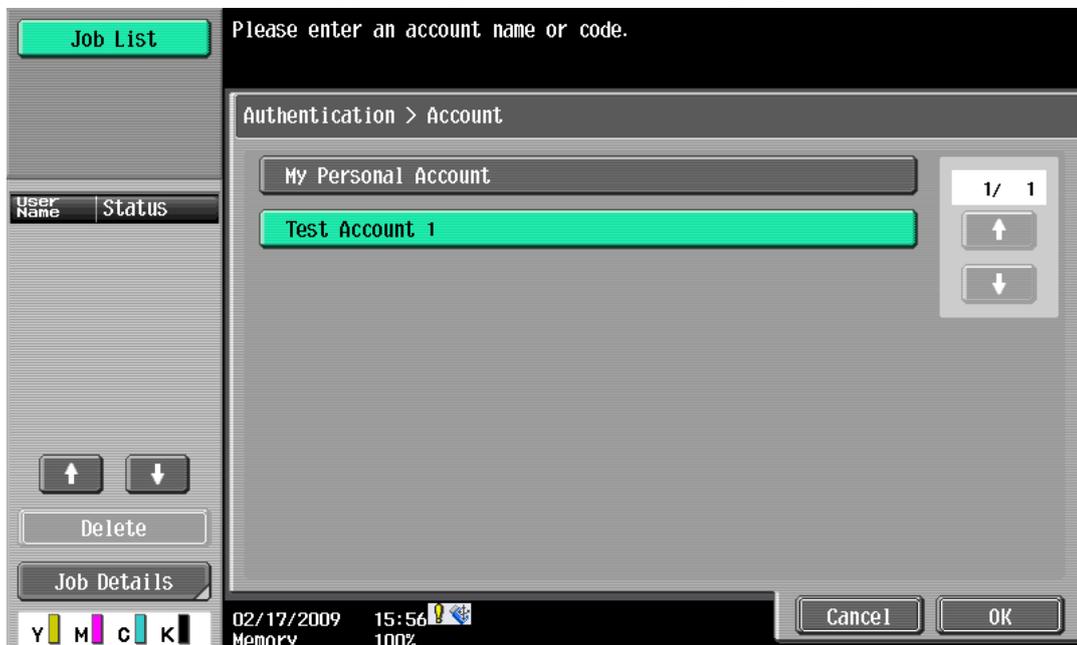
Firstly a test account should be created:

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”.

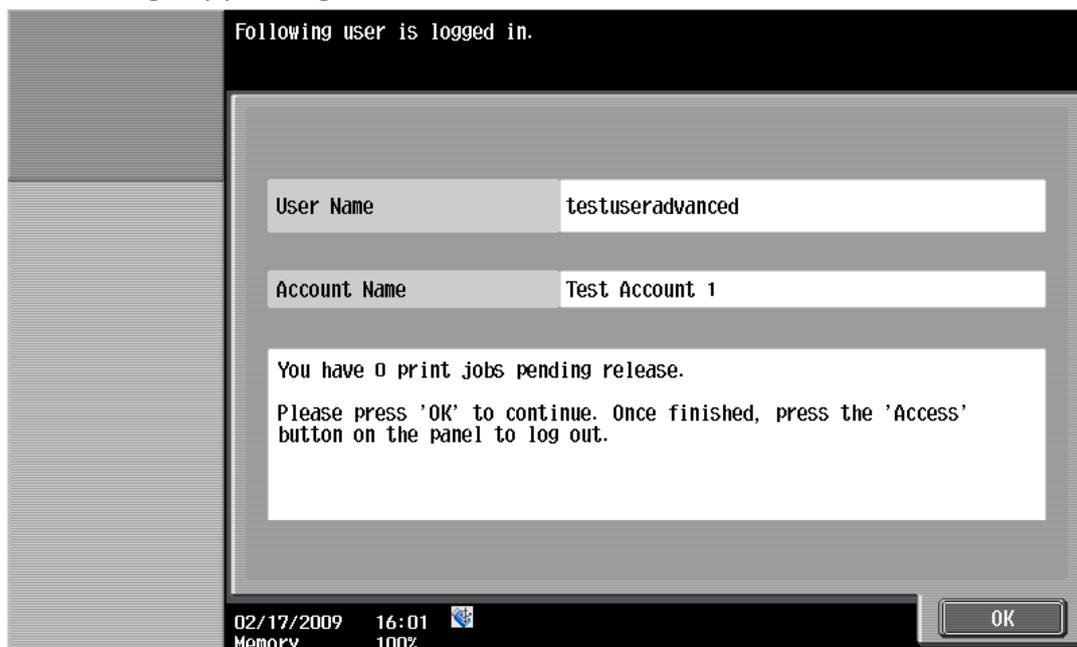
At the photocopier:

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 release stations, 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 release station” 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.

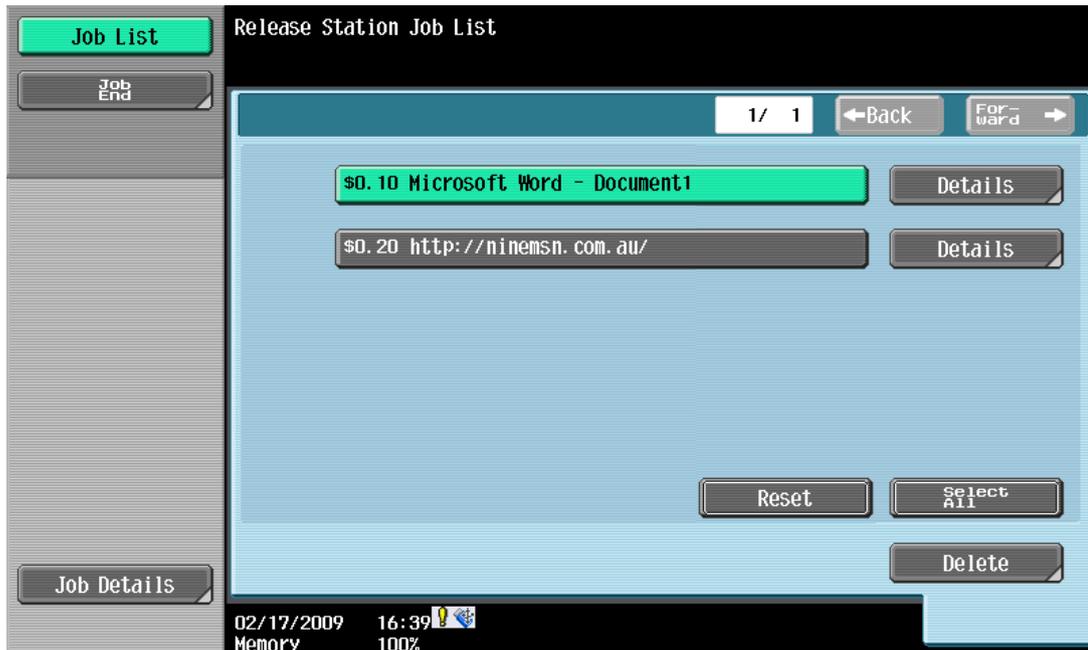


5. Press “OK” to save.
6. Login to a computer workstation as ‘testusersimple’.
7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
8. Confirm that the jobs are held, by checking that the jobs are listed in the “Printers -> Jobs Pending Release”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

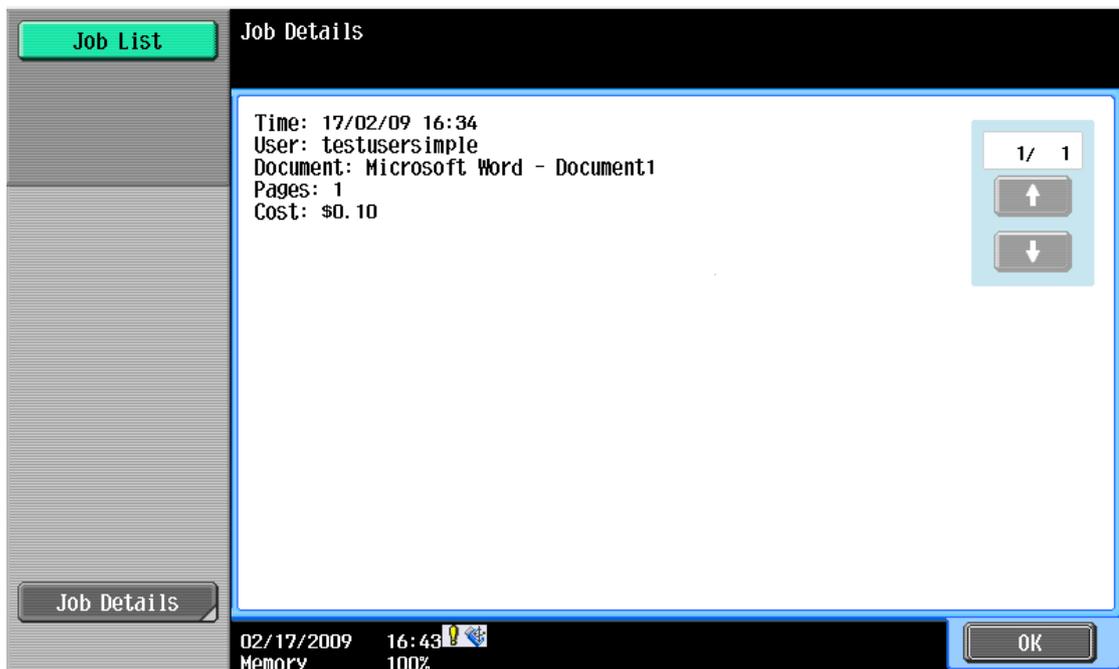
At the device:

5. Log in with the ‘testusersimple’ username and corresponding password as in scenario 1.
6. 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.

- Press the “Release” button on the left of the screen. A list of print jobs will show. You can highlight and unhighlight individual items by pressing the list item:

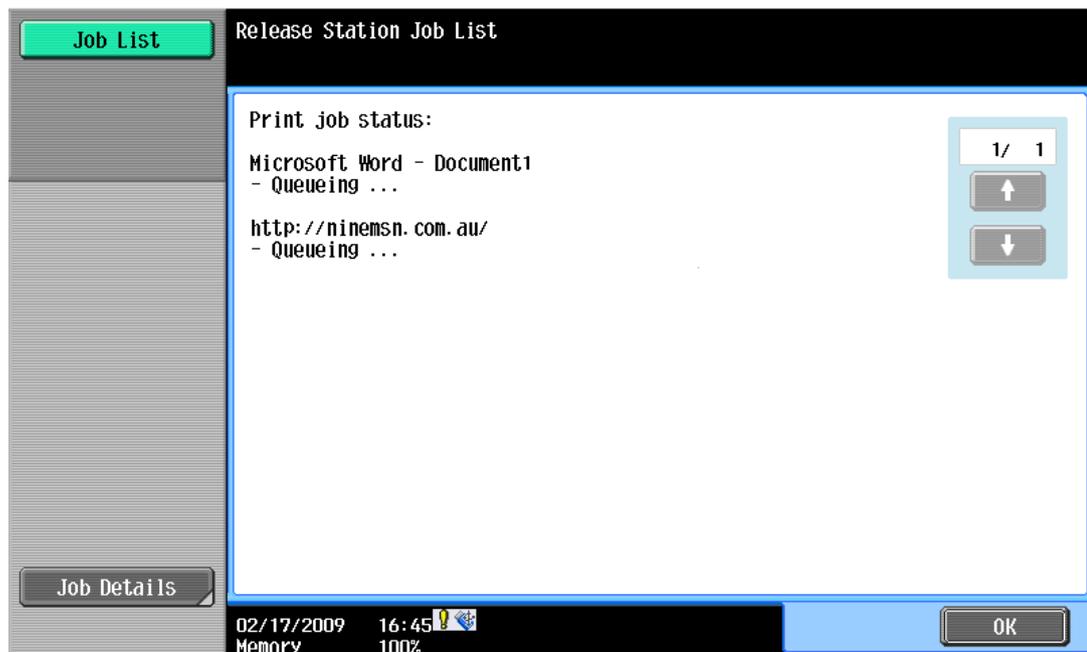


- Press the “Details” button next to a list item to display details about the print job. Go back with “OK”.



- 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.



10. Dismiss the confirmation by pressing “OK”. This will take you back to the list of print jobs which may now be empty.
11. 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”.
12. Finish releasing or deleting jobs by pressing “Job End” at the top left of the screen.
13. 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.

<input checked="" type="checkbox"/>	Track & control scanning
Charging type	
	advanced ▾
Page cost	\$0.10
Page cost after threshold	\$0.05
Page count threshold	1
<input checked="" type="checkbox"/>	Track & control faxing
Charging type	
	advanced ▾
Page cost	\$0.20
Page cost after threshold	\$0.10
Page count threshold	1

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:

4. Log in to the PaperCut administration interface.
5. Select the device from the "Devices" tab.
6. 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.

<u>Usage Date</u> ▼	<u>User</u>	<u>Charged To</u>	<u>Pages</u>	<u>Cost</u>	<u>Document Name</u>	<u>Attrib</u>
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]	

7. Click on the user's name in the user column to view the user's account details.
8. Select the "Job log" tab to display all activity for the user.
9. 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.

Device function (e.g. copy, release station or both)

Track & control copying

Page cost

(simple)

Track & control scanning

Track & control faxing

Enable release station

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 release station	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

Username and password

Identity number

Require PIN

Swipe card

Automatically login as user

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 user	Specifies that this device should always automatically log in as the given 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 'Config Editor (Advanced)' tab.

Config name	Description
ext-device.konica-minolta.message.welcome.line1	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

and ext-device.konica-minolta.message.welcome.line2	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.appno.auth and ext-device.konica-minolta.appno.pullprint	Some Konica Minolta devices may have other embedded applications installed such as “Pull Print” applications that allow easy access to print documents from a repository of often-printed documents. These applications occupy “application slots” in the device numbered from 1 to 10 or higher and may conflict with PaperCut which by default occupies slots 1 and 2. If either slot is occupied by another application, change the value to a free slot here.
ext-device.konica-minolta.login.confirmation.enabled	Setting this to “N” allows you to bypass the confirmation screen shown after a successful login.
ext-device.card-no-regex	See chapter 5.4 “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.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. 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 the PaperCut administrator interface or the server is restarted. Must be set back to “N” to apply settings. Use with care.

5.2 Additional options for OpenAPI 2.3 devices

ext-device.konica-	Setting this to “N” will remove the account field from the “Authentication”
--------------------	---

minolta.login.show-account	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	<p>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.</p> <p>Default for ext-device. konica-minolta.limit-reference.duplex: N (No)</p> <p>Default for ext-device. konica-minolta.limit-reference.paper-size in North America: Letter</p> <p>Default for ext-device. konica-minolta.limit-reference.paper-size worldwide: A4</p>
ext-device.konica-minolta.paper-size.regular and ext-device.konica-minolta.paper-size.large	<p>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.</p> <p>The "regular" size should be equal to "ext-device.konica-minolta.limit-reference.paper-size" above for accurate accounting.</p>
ext-device.konica-minolta.duplex.detection	Optionally switch off duplex detection. Duplex detection is subject to limitations as discussed in chapter 7.7.3 "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).

5.3 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 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 you can 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.

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

5.4 Configuring Swipe Card Readers

At the time of writing Konica Minolta devices only support the following reader types

1. The "AU-201" which is a Mifare/Type-A reader.
2. The Omnikey CardMan series of HID readers.

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.

Swipe cards contain numbers which are used to identify users according to the card number configured in the User Details screen under "Card/Identity" number. Some readers report information in addition to the number encoded on the card, such as checksums. PaperCut can treat these cases in two ways:

- A typical case is the checksum being reported after the card number, separated by an equals sign, such as in 5235092385=8. PaperCut can handle this case by default; it will extract the number before the equal sign as the card number: 5235092385.
- For some cases, a "regular expression" *may* be required that will filter the card number from the complete string of characters reported by the card reader. Documentation on regular expressions can be found on the Internet, e.g. at www.regular-expressions.info.
 - The regular expression must be fashioned so that the card number is returned as the first match group.
 - Usually one regular expression will be used for all the devices managed by PaperCut; this must be entered in the "Config editor (advanced)" which you will find on the Options tab under Actions. The key is called "ext-device.card-no-regex".
 - The global setting however can be overridden on a per-device basis: The key "ext-device.card-no-regex" can also be found on the "Config Editor (Advanced)" tab in the device details screen. This setting will override the global setting unless the keyword "GLOBAL" is specified.
 - PaperCut developers will gladly assist in producing a regular expression when supplied with a few sample outputs from your card reader. Please contact PaperCut support.

- If you would like to write your own regular expressions, here are some examples:
 - Use the first 10 characters (any character): `(. {10})`
 - Use the first 19 digits: `(\d{19})`
 - Extract the digits from between the two “=” characters in “123453=292929=1221”: `\d*=(\d*)=\d*`

5.5 Card Self-Association

Card self-association allows users to associate their card, or a new card with this domain account directly at the device. The process works as follows:

1. The user swipes a card not known to PaperCut at a device with card self-association enabled.
2. The device gives the user the option to associate the card with their account
3. The user logs in again, this time adding their username and password in the appropriate fields.
4. If the username and password match a valid domain username and password, the card number is remembered and associated with this user thereafter – the user may use this card to access devices without requiring entering username and password.

6 Uninstalling

In order to remove PaperCut authentication and release station 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:

- No ability to search accounts by keyword.
- The 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 to many key presses.

7.2 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.

7.3 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.

7.4 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.

7.5 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 searching accounts by keyword and adding comments and invoicing options to jobs
- Limits on the length of print job names displayed

7.6 USB printing and scanning

Installing PaperCut has shown to disable USB printing and scanning on at least some devices. Consider your requirements for USB printing and scanning before installing PaperCut on a Konica Minolta machine.

7.7 Additional Limitations for OpenAPI 2.3 devices

7.7.1 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.

7.7.2 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.

7.7.3 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 ...”?

This message should not appear for more than a few seconds; however some Konica Minolta devices exhibit instability and stop responding at this point. Please check whether the device’s network connection is functional and check the device status in the PaperCut web administration interface. If no other cause can be found, switch the device off for 5 seconds and switch it on again.

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.

Appendix A: Setup and operation on older OpenAPI 2.3 models

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>/`. Tip: The default administrator's password usually is "12345678".
- 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-logout 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.

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.

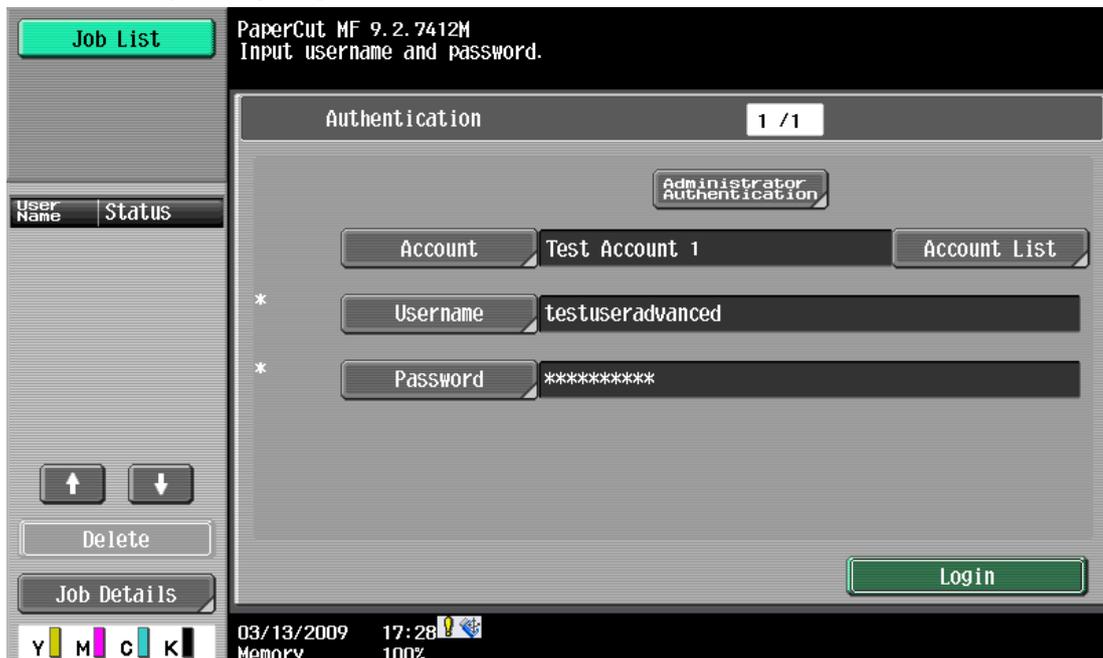
System administrators are encouraged to read the following information, familiarize themselves with the scenarios and educate their users as to the correct operation of account selection.

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.



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.