PaperCut MF - Konica Minolta i-Option Embedded Manual

Contents

QRDOC.IO

20231208

1 Document revision history

Published date or release	Details of changes made
2023-05-30	2.3.2 Configure SSL Certificate Verification Errors
21.1	5.15 Phonebook contacts, 8 Appendix A Device Screens
19.2.0	2.3.4 Install PaperCut MF
19.1.4	4.10 Config Editor; 5.13 Impact of Advanced Charging on Integrated Scanning
19.1.0	3.3.2 Web Browser Configuration; 5 Configuration; 7 Known Limitations
19.0.0	2 Overview; 5.3 Language selection at the device; 5.8 Held print job settings at the device; 5.13 Config Editor
18.3.6	5.4 "Swipe card" authentication method
18.3.5	5.12 Config Editor; 7.13 JPG, TIFF Integrated Scan jobs on compact devices are always in portrait mode
18.3.3	5.12 Config Editor
18.3.0	3.2 Requirements; 3.3.4 Install PaperCut MF; 5.8 PaperCut MF's Integrated Scanning; 5.12 Config Editor; 7 Known Limitations; 8 FAQ & Troubleshooting; 9 Appendix A: Device screens
18.2.4	5.6 Device functions; 5.11.1 Header colors; 5.12 Config Editor; 7 Known Limitations
18.2.3	7 Known Limitations
18.2.0	2 Overview; 3 Installation; 4 Post-install testing; 5 Configuration; 7 Known Limitations; 9 Appendix A: Device screens

18.1.4	5.3.4 Install PaperCut MF; 7.12 Config Editor; 9.13 SHA1 warning message
18.1.1	8.1 Config Editor

2 Installation

This section covers the installation of the PaperCut embedded application for compatible Konica Minolta MFDs. The embedded application will enable MFD access control, secure printing and "Find-Me" printing, and allow logging and control copying, scanning and faxing. For information on just tracking network printing see the PaperCut user manual.

2.1 Supported devices

Ensure that the Konica Minolta i-Option OpenAPI devices running compatible web browsers are listed as supported devices on the <u>PaperCut MF for Konica Minolta</u> page.

Note: PaperCut MF 18.2.0 or above does not support Konica Minolta i-Option OpenAPI devices running the NetFront Browser. For more information, see 5.14 PaperCut MF 18.2.0 or above does not support Konica Minolta i-Option OpenAPI devices running the NetFront browser .

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 devices with a hard drive installed. - LK101 upgrade kit may be required from Konica Minolta - A web browser (depending on MFP model)	Yes
Konica Minolta (OpenAPI 4.0+)	Yes - 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

2.2 Requirements

Before installing the PaperCut Embedded Application on to 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 3.1 or later.
- Ensure that the Konica Minolta device is connected to the network.
- Have available the network name or IP address of the Konica Minolta device.
- It is recommended that the device be configured with a *static IP address*.

- Verify that firewalls or other network restrictions do not prevent the PaperCut server's access to port 50003 on the device and do not prevent the device's access to the PaperCut server on ports 9191, 9192 and 9195 (PaperCut MF 18.3.0 or above).
- Ensure the device has a Web browser installed and activated. You can check that the "web browser" is listed under 'Administrator Settings > License Settings > List of Enabled functions' on the device.

2.2.1 Integrated Scanning

The PaperCut MF embedded application includes Integrated Scanning, which you can optionally enable per device. Integrated scanning has the following additional requirements:

- Firmware must support OpenAPI version 4.0+
- Requires i-Option device

2.3 Setup Procedure

To install PaperCut MF (i.e. device registration and integration):

- 2.3.1 Configure OpenAPI Settings

- 2.3.2 Configure SSL Certificate

- 2.3.3 Web Browser Configuration

- 2.3.4 Enabling Unauthenticated Printing

- 2.3.5 Install PaperCut MF

    - 2.3.5.1 Install PaperCut MF on multiple devices

    - 2.3.5.2 Install PaperCut MF on each device

- 2.3.6 Add the PaperCut Release and Scan icons to the main menu

2.3.1 Configure OpenAPI Settings

1. Log on as administrator on the device's web interface (called "Page Scope Web Connection") under http:// <ip-address-of-device>/ ."
2. 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.
3. 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.)
    a. Click "New Registration", select "Create and register a self-signed Certificate" and click "OK".
    b. Fill in the fields with some values about your organization. The values have no functional significance.
    c. For the "Validity Period", the maximum number of days offered is recommended (usually 3650 = 10 years).
    d. "Encryption Strength" can be left to the default values.

     e.   Click "OK". The certificate will be generated. You will be asked to switch the device off and on again.

4. Log into the device web interface as administrator again. 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.

5. Optional: 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". Keep a record of the password in a safe place, as per normal system management best practice.

6. 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.

7. Log back into the administrator web interface, and in the "Network" section display the "OpenAPI" subsection.
     a.   In the "Use SSL/TLS" drop-down list, select "SSL Only".
     b.   Make sure the "Port No. (SSL)" is set to 50003.
     c.   Click "OK".

8. Some newer devices include an OpenAPI password that needs to be removed. To do so, access the administrator settings on the device's panel, not the web interface:
     a.   Press the "Utility" button on the button panel.
     b.   Press "Administrator Settings" on the screen.
     c.   Log in with the administrator password.
     d.   Selection "System Connection" > "OpenAPI Settings" > "Authentication".
     e.   Make sure "OFF" is selected and press "OK".

9. For security reasons it is also recommended to change the device's default administrator web access password.

10. Ensure SSDP protocol is enabled under Utility > Administrator > Settings > Network Settings > SSDP Settings.

11. Ensure WebDAV server is enabled on the device (under Administrator Settings > WebDAV Settings > WebDAV Server Setting). Port 80 on the device will need to be accessible from the PaperCut application server in order to push out application resources over WebDAV.

12. When MFD is configured for access check you can access the following URL: http://<MFP IP>/OpenAPI/DeviceDescription/ from the same network location where PaperCut server is deployed, where HOSTNAME is the hostname or IP address of the MFD. If accessed with your web browser the operation should complete successfully and an XML document published by the MFD be displayed.

13. Check that the web browser is activated on the device prior to proceeding further. The way in which you do this differs between models. One example is shown below:
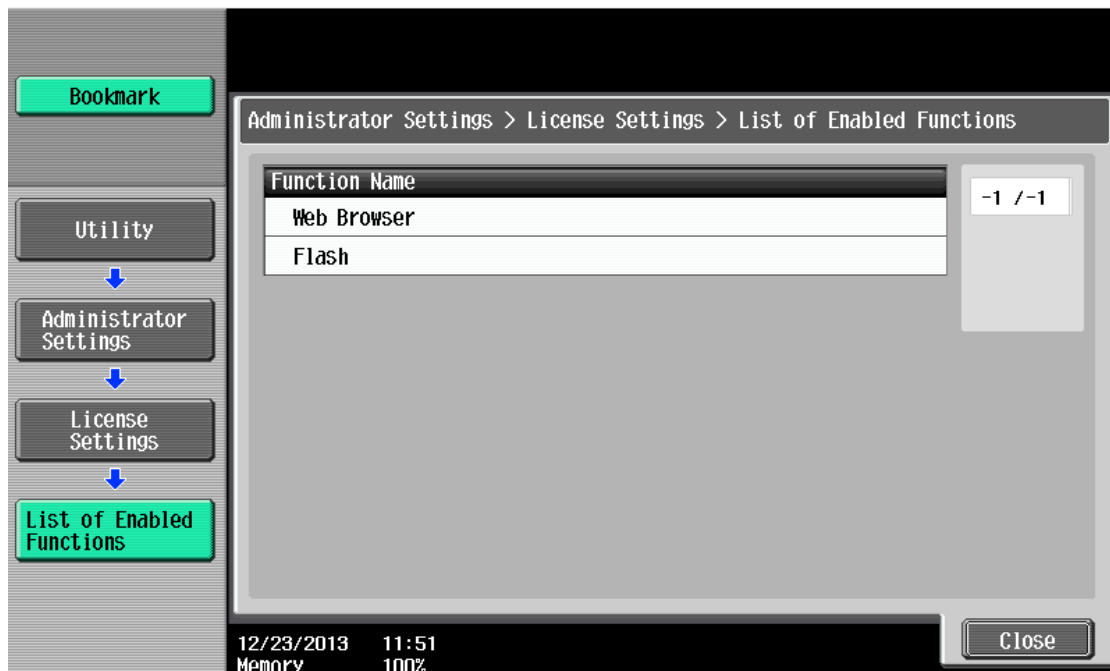
If "Web Browser" is not listed, you will need to contact your Konica Minolta dealer and obtain the LK101 upgrade kit and install the browser license on each of your devices (via Install License function in the License Settings).

2.3.2 Configure SSL Certificate

If you are using HTTPS to secure the communication between device and PaperCut MF server, review if your CA or self-signed certificate contains complete information.

If you don't have the complete information in place, you will see the warning mentioned in 4.2.1.5 Certificate registration warnings.

If you are using a Certificate Authority-signed certificate, refer to 4.2.1.1 Certificate Authority signed certificate. If you are using a self-signed certificate, refer to 4.2.1.2 Self-signed certificate.

2.3.3 Web Browser Configuration

Ensure the web browser on the device has SSL/TLS connections and JavaScript enabled (under web browser settings).
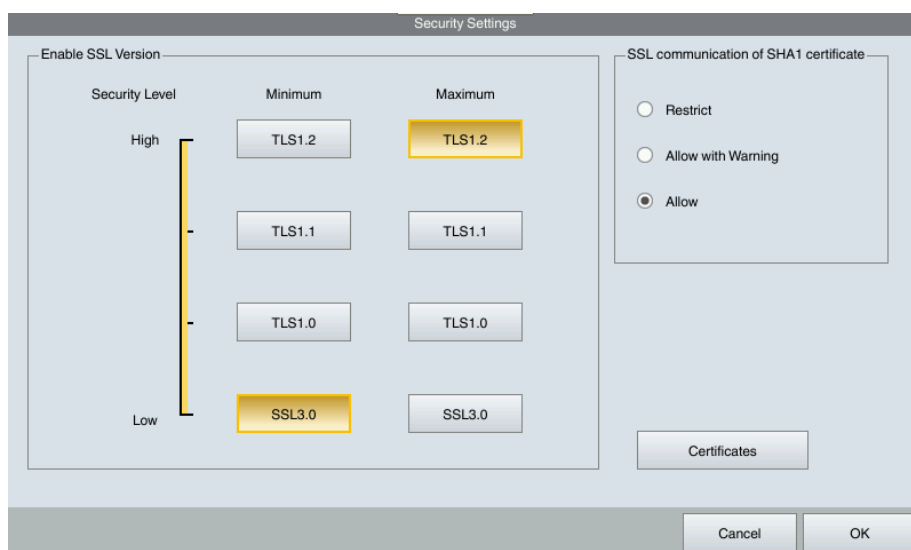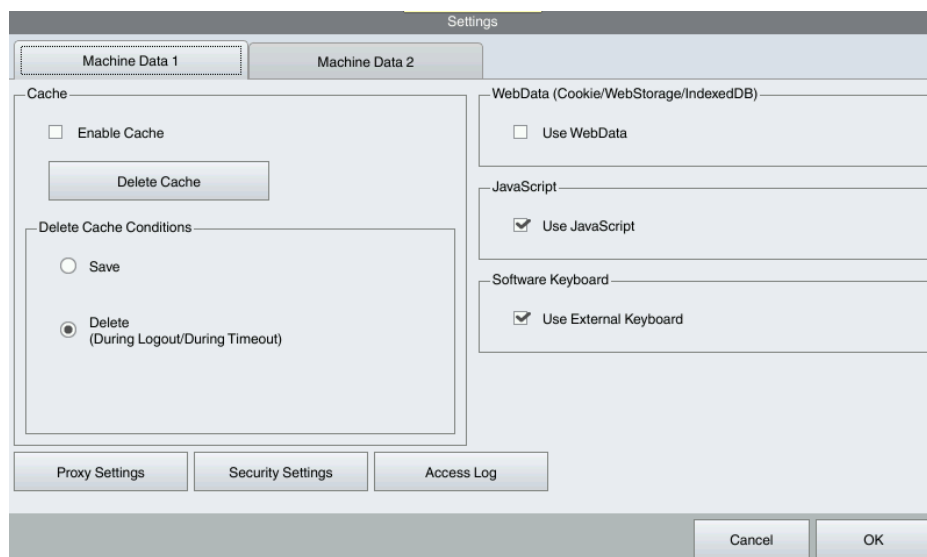
This requires manually starting the browser application to confirm the settings are okay. The location of the settings may differ slightly on different models.

2.3.4 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 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:

1. Click "Acquire Settings". Make sure the "Auto" check box is **not** selected. Click "OK".
   o 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 device.

2. At the top right of the "Configure" tab, in the "Device Option" list, scroll down to "User Authentication" and select "Disable".
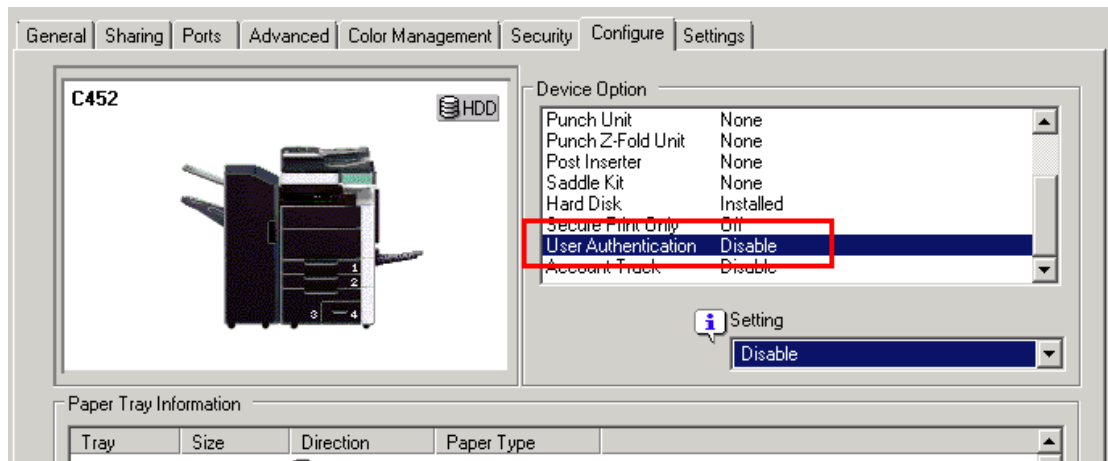
3. Close the Properties window by clicking "OK".

For other operating systems, please consult your Konica documentation.

NOTE: If you are using a virtual queue for load balancing/"find me" printing, then apply the same setting to the virtual queue as well.

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:

1. Press the "Utility/Counter" button.
2. Select "Administrator Settings". Enter your administrator password and press "OK".
3. Select "User Authentication/Account Track".
4. Select "Print without Authentication".
5. Select "Allow".
6. Select "OK".

For configuration via the web interface:

1. Open the device's IP address or hostname in a web browser.
2. Log in as the Administrator.
3. Select Security -> Authentication -> General Settings.
4. Set "Public Access" to "Restrict".
5. Set "Print without Authentication" to "Allow".
6. Select "Apply".

Alternatively, on some copiers it's found via:

1. Open the device's IP address or hostname in a web browser.
2. Log in as the Administrator.
3. Select User/Auth/Account Track.
4. Select Print without Authentication
5. Set "Print without Authentication" to "Full Color/Black"

Maintenance	System Settings	Security	User Auth/Account Track	Network	Box

Print Setting	Store Address	Fax Settings	Wizard	Customize	To Main Menu

▶ General Settings

▶ Prohibited Function Login Setting

▶ Print without Authentication

▶ Simple Print Authentication Setting

▶ External Server Settings

▶ Public User Box Setting

▶ User/Account Common Setting

▶ Scan to Home Settings

▶ Scan to Authorized Folder Settings

▶ Authentication Card ID Number

Print without Authentication

| Print without Authentication | Full Color/Black |
| IP Filtering (Permit Access) | Disable |

IP Address

Range1	0.0.0.0	-	0.0.0.0
Range2	0.0.0.0	-	0.0.0.0
Range3	0.0.0.0	-	0.0.0.0
Range4	0.0.0.0	-	0.0.0.0
Range5	0.0.0.0	-	0.0.0.0

OK   Cancel

2.3.5 Install PaperCut MF

To install PaperCut MF (i.e. device registration and integration):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **External Hardware Integration** area, select **Enable external hardware integration (for supported devices only)**.
4. Click **Apply**.
5. You can use any one of the following options:

   - 2.3.5.1 Install PaperCut MF on multiple devices

   - 2.3.5.2 Install PaperCut MF on each device

2.3.5.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 introduced a feature to create multiple devices in bulk through a CSV file via server commands. In 20.0.0 we added a way to load this CSV file via the PaperCut MF UI. You can find the feature under: PaperCut MF > Devices > Create multiple devices.
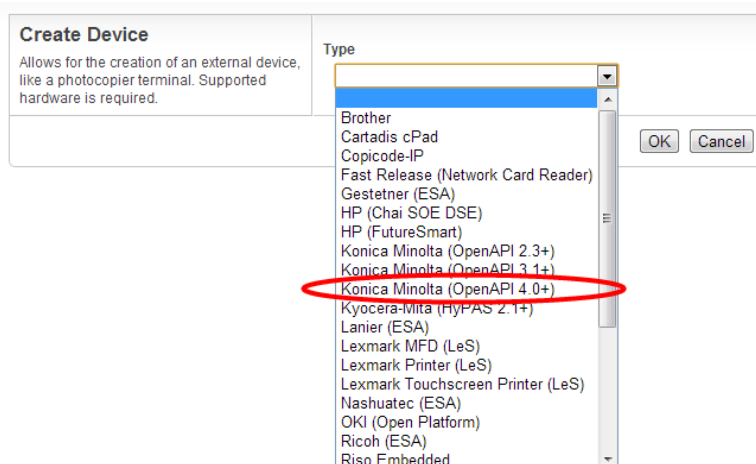
Using this feature increases your operational efficiency by significantly reducing the time taken to add devices to PaperCut MF. From version 20.0, this feature also allows for you to add devices to PaperCut MF before such devices are delivered to their installation site, such devices are added with a "Staged" status. The scenario for "Staged" devices applies when the system admin already knows all the device's attributes prior to its delivery. For more information, see the Enhanced Deployment Project.

2.3.5.2 Install PaperCut MF on each device

Note: If you are running a version prior to PaperCut MF 19.2.0, then this is the only applicable option.

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**
4. In **Type**, select the applicable **Konica Minolta** option:

Note: To enable Integrated Scanning, select **Konica Minolta (OPenAPI 4.0+).**

5. In **Device name**, enter a descriptive name for the device.

6. Optionally, in **Location/Department**, enter location or department details of the device.

7. In **Hostname / IP**, enter the network name or IP address of the device.

8. In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device's web interface.

9. In **Function**, select the relevant device jobs:

   - **Track & control copying**
   - **Track & control scanning**
   - **Track & control faxing**
   - **Enable print release**

   Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.
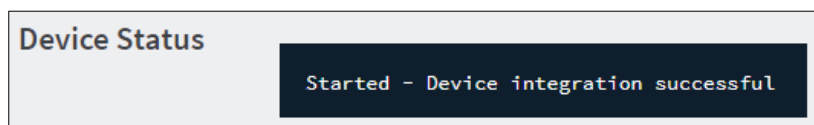
10. Click **Ok**.

    PaperCut MF's installation on the device (i.e. device registration and integration) starts:

    Device Status

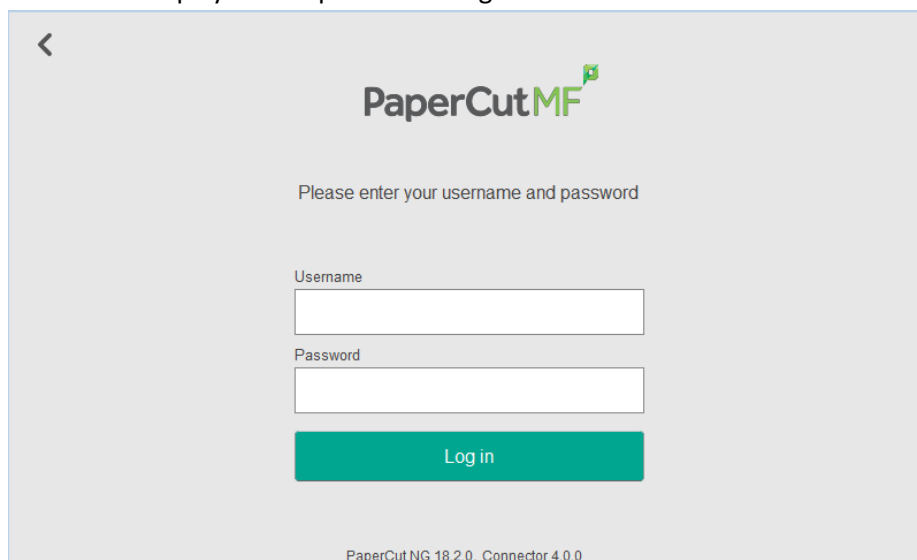   Started - Setting up device integration
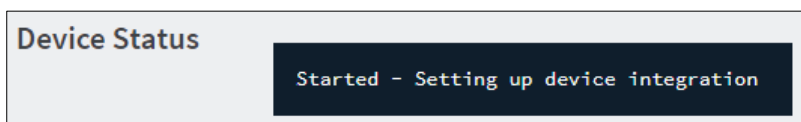
11. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):

    - The **Device Status** displays the status **Started – Device integration successful**:

      Device Status

      Started - Device integration successful

    - The device displays the PaperCut MF Login screen:

      PaperCut MF

      Please enter your username and password

      Username

      Password

      Log in

      PaperCut NG 18.2.0, Connector 4.0.0

    Note: Based on the version of PaperCut MF being installed, the following could apply, resulting in required actions:

    - If you are upgrading to 18.3 or above, the following warning message is displayed on the:
      - PaperCut MF Admin web interface:

        ⚠ Communication with this device is using weak SHA1-based encryption for SSL/TLS communications. To configure it to use stronger encryption, please set advanced config key ext-device.konica-minolta.use-high-security-port to "Y".
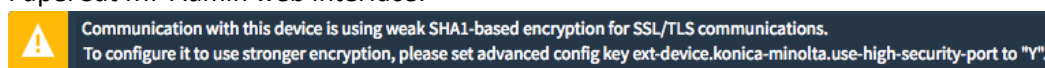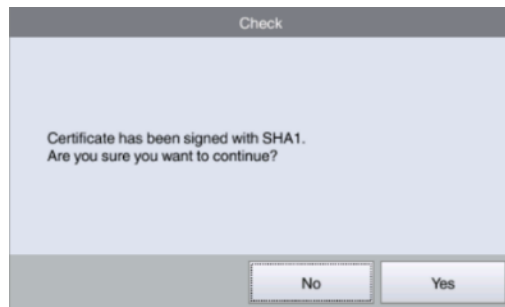
      - device:

For more information, see 4.2.1.3 SHA 1 warning message on PaperCut MF 18.3 or above

- If you are upgrading to 18.2.6 or below, the following warning message is displayed on the:
    - PaperCut MF Admin web interface:

> ⚠ PaperCut is currently configured to use a SHA1 encrypted certificate for SSL/TLS communications.
> This can affect the functionality of some Konica Minolta devices.
> Please refer to this Knowledge Base article on the PaperCut website for more details, or contact your reseller or ASC.
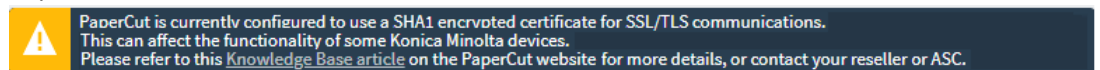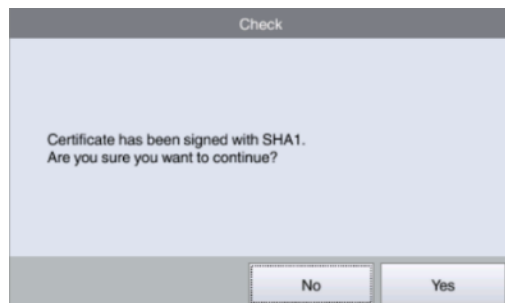
    - device:

For more information, see 4.2.1.4 SHA 1 warning message on PaperCut MF 18.2.6 or below

## 2.3.6 Add the PaperCut Release and Scan icons to the main menu

Note: For models with OpenAPI 4.1+, a config key is available to add the Release and Scan icons to the main menu. You need to manually add these icons only for devices earlier than OpenAPI 4.1.

The device main menu does not automatically display the PaperCut icons. You can reposition the existing native Copy and Scan/Fax icons with the PaperCut icons so they are displayed first on the main menu screen.

After you have installed Papercut MF with Print Release and/or Integrated Scanning:

1. Login to the device
2. On the device main menu, press "Utility".
3. Press "Administrator Settings".
4. Enter the administrator password; then press "OK".

5. Press "System Settings".
6. Press "Custom Display Settings".
7. Press "Default Bypass Paper Type Setting".
8. Press "Custom Display Settings".
9. Press "Main Menu Default Settings".
10. Replace the device Copy icon with the Papercut Release icon:
    a. Press "Main Menu Key 1 (Copy)".
    b. Press "Registered Application".

    c.   Select "Release"; then press "OK".
        The Main Menu Default Settings page is displayed with the Main Menu Key 1 changed to Release.

11. Replace the device Scan/Fax icon with the PaperCut Scan icon:
    a.   Press "Main Menu Key 2 (Scan/Fax)".
    b.   Press "Registered Application".
    c.   Select "Scan"; then press "OK".
        The Main Menu Default Settings page is displayed with the Main Menu Key 2 changed to Scan.

12. Add the native device Copy icon:
    a.   Press "Main Menu Key 5 (Do not use)".
    b.   Press "On".
    c.   Press "Function".
    d.   Select "Copy"; then press "OK".
        The Main Menu Default Settings page is displayed with the Main Menu Key 5 changed to Copy.

13. Add the native device Scan/Fax icon:
    a.   Press "Main Menu Key 6 (Do not use)".
    b.   Press "On".
    c.   Press "Function".
    d.   Select "Scan/Fax"; then press "OK".
        The Main Menu Default Settings page is displayed with the Main Menu Key 5 changed to Copy.

14. Close the Administrator Settings window. Next time a user logs in to the device, they will see the native screen.
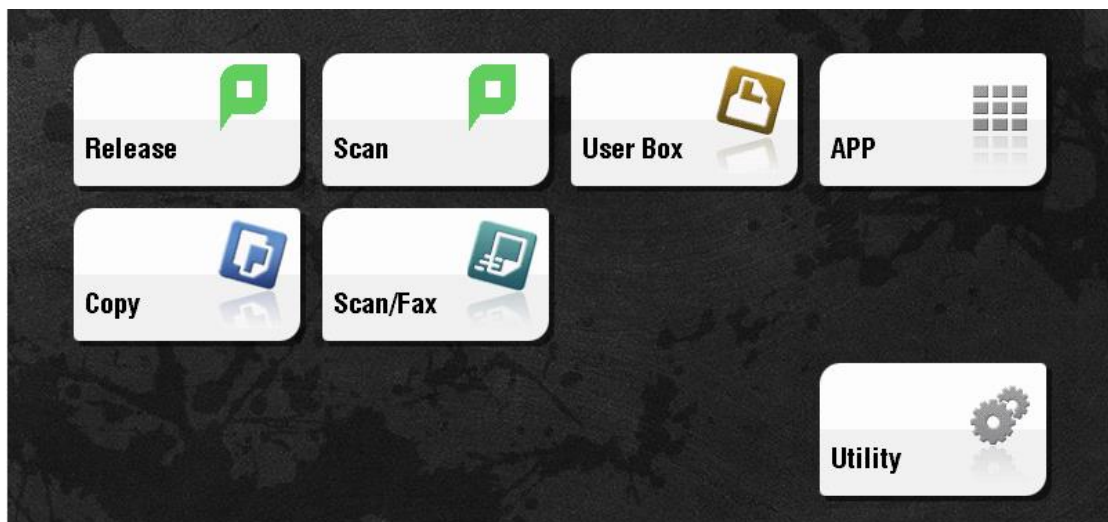
If you remove the PaperCut MF icons from the main menu or uninstall PaperCut MF, the PaperCut icons will automatically be replaced with the device native icons, leaving duplicate icons on your menu. You need to remove the device native icons (Copy and Scan/Fax) that you previously manually added, so that only the default icons are displayed.

1. Login to the device
2. On the device main menu, press "Utility".
3. Press "Administrator Settings".
4. Enter the administrator password; then press "OK".

5. Press "System Settings".
6. Press "Custom Display Settings".
7. Press "Default Bypass Paper Type Setting".
8. Press "Custom Display Settings".
9. Press "Main Menu Default Settings".
10. Remove the manually added Copy icon:
    a. Press "Main Menu Key 5 (Copy)".
    b. Press "Off".
11. Remove the manually added Scan/Fax icon:
    a. Press "Main Menu Key 6 (Scan/Fax)".
    b. Press "Off".
12. Close the Administrator Settings window. The manually added device icons are no longer displayed in the main menu.

2.4 Upgrading to a newer version

The PaperCut Konica Minolta Embedded will be up to date when you upgrade your PaperCut installation; no further action is necessary.

When upgrading from a standard UI version of the embedded software (OpenAPI 3.1) for the first time, the web based interface will not be enabled by default unless a new device is created.

To enable this for an existing device set ext-device.konica-minolta.browser.enabled to "Y" under the advanced configuration tab of the device details screen. See section 4.10.

To force all i-Option capable Konica devices to use the standard UI set ext-device.konica-minolta.browser.enabled to "N". See section 4.10.

Generally, the configuration settings such as whether the browser is to be enabled will not be touched after upgrade so once it's set one way or another it will be retained unless explicitly changed by the administrator in PaperCut.

3 Post-install testing

After PaperCut MF is installed on the device (i.e. device registration and integration is completed), it is recommended that you test some common usage scenarios. This is important for two reasons:

- To ensure that PaperCut MF works as expected.
- To familiarize yourself with the features and functionality of PaperCut MF.

This section covers the following post-install testing scenarios devices that support i-Option OpenAPI 3.1 or higher.

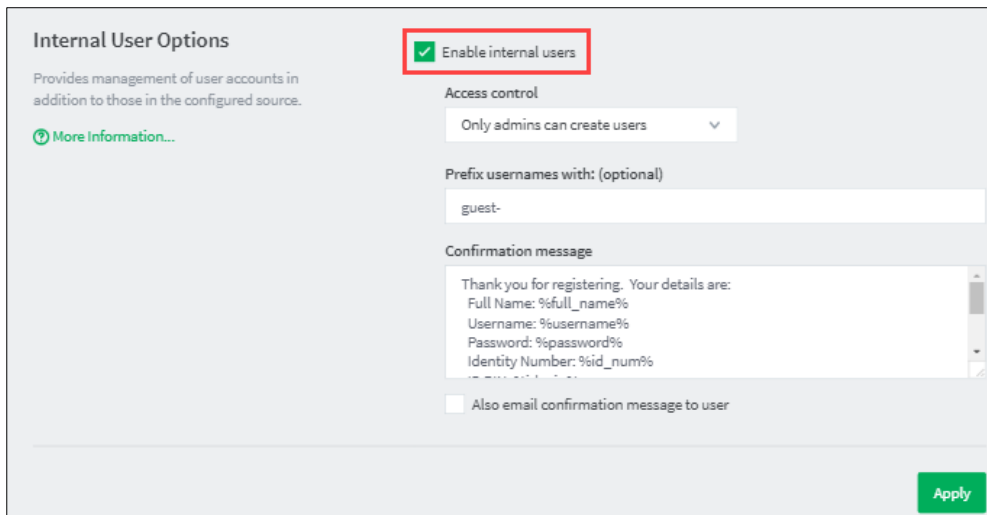- 3.2 Simple printing and copying

- 3.3 Advanced copying

3.1 Test preparation: create test users

To execute the post-install testing scenarios, ensure at least two test users are created:

- **Simple test user** – A user who performs simple printing and copying.
- **Advanced test user** – A user who performs advanced copying.
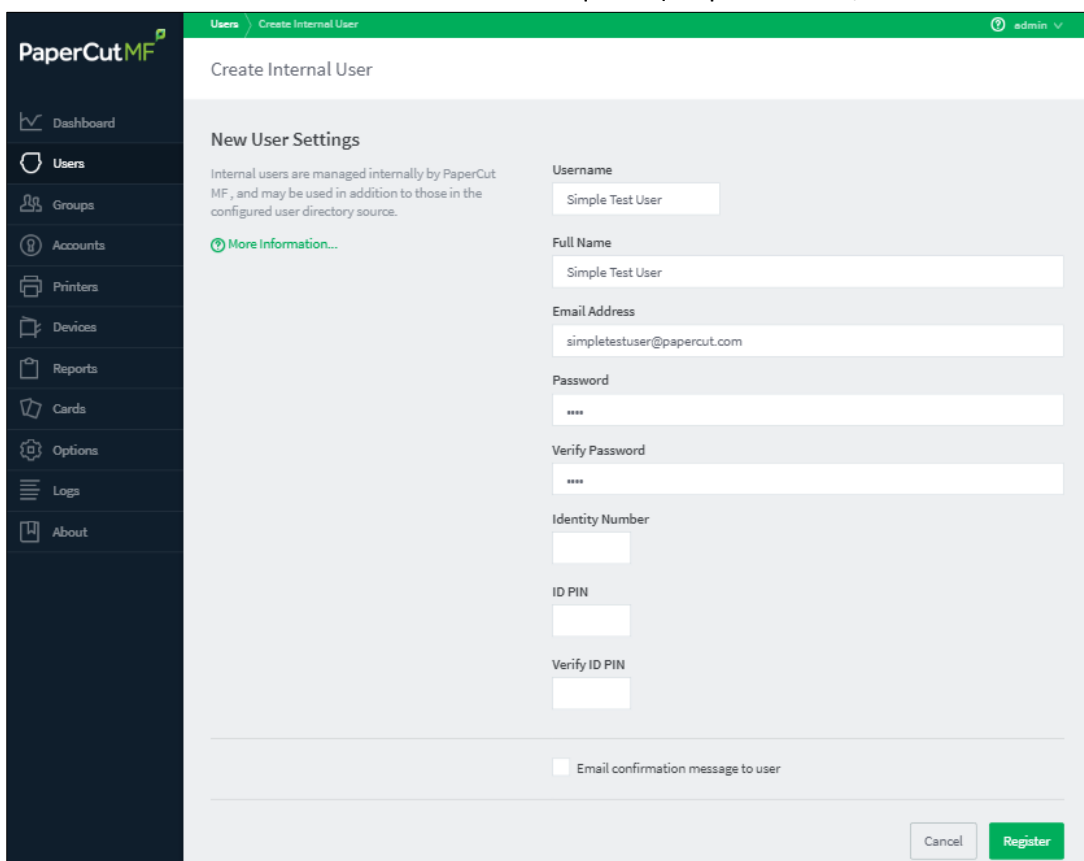
To create test users:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > User/Group Sync**.
3. In **Internal User Options**, select **Enable internal users**.
4. Click **Apply**.

5. Navigate to **Users**.
6. Click **Create internal user…**
7. Enter the relevant details for the test users as required (simple test user, advanced test user):
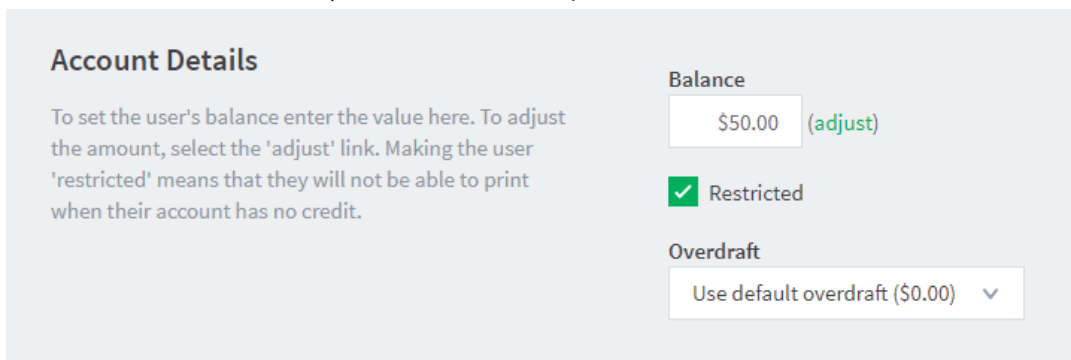
8. Click **Register**.

3.2 Simple printing and copying

3.2.1 Test preparation: configure simple test user
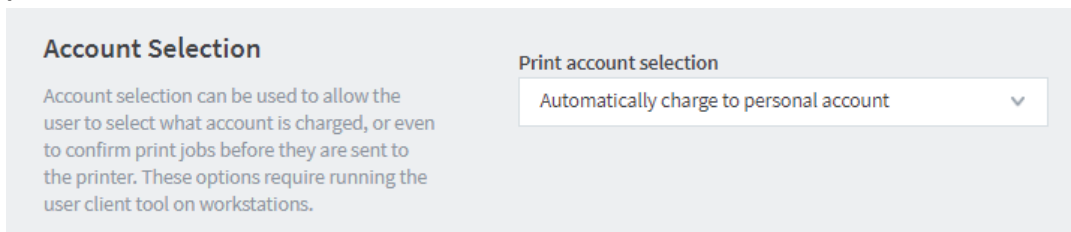
To test the simple test scenarios, ensure at least one simple test user is created. For more information, see 3.1 Test preparation: create test users. Once created, ensure the simple test user is configured.

To configure the simple test user:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Users**.
3. From the **User List**, select the simple test user.
4. In the **Account Details** area, set the **Balance** to **$50.00** and select **Restricted:**

5. In the **Account Selection** area's **Print account selection**, select **Automatically charge to personal account**:

6. Click **Apply**.

3.2.2 Simple printing

Simple printing does not involve providing the simple test user with a choice of accounts to choose from. Printing is charged to the simple test user's default My Personal Account.

To test simple printing, ensure the following test preparation requirements are met:

- **Simple test user** - A simple test user is created and configured. For more information, see 3.1 Test preparation: create test users and 3.2.1 Test preparation: configure simple test user.
- **Printer queue settings** - The printer queue's Hold/Release Queue Settings are configured. For more information, see the PaperCut MF manual.
  To configure the printer queue's Hold/Release Queue Settings:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Printers**.
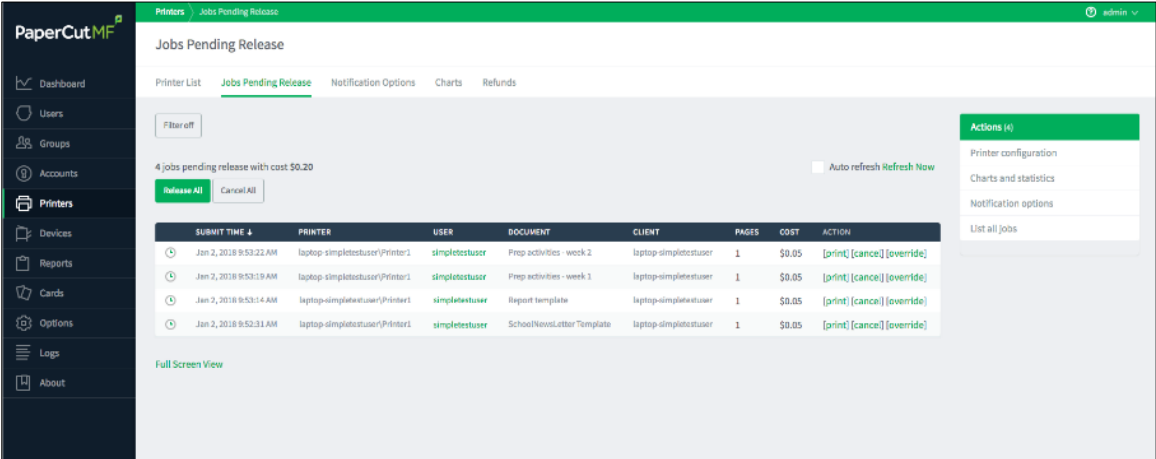
3. Select the Printer that is applicable to the device being tested.

4. In the **Hold/Release Queue Settings** area, select the **Enable hold/release queue**.

5. Click **Apply**.

   Print jobs to this printer queue are held until released by a user.

- **Device functions** – Printing is enabled. To enable printing:

  1. Log in to the PaperCut MF Admin web interface.

  2. Navigate to **Devices**.

  3. Select the device being tested.

  4. In the **Print Release** area, select **Enable print release**.

  5. In the **This device will display jobs for release from the selected source queues**, select at least one source queue for print release that corresponds to this device's configured printer queue.

  6. Click **Apply**.

  7. Verify that the **Devices > External Device List** displays the device with **Print Release** in the **Function** column.

To test simple printing:

1. Log in to a computer as the simple test user.

2. Print a few jobs to the source queue that was selected in the **Devices > External Device List > Device Details > Print Release > Enable print release** area of the device being tested.

3. Log in to the PaperCut MF Admin web interface.

4. Navigate to **Printers > Jobs Pending Release**.

5. Verify that the print jobs for the simple test user are being held and listed:

6. Log out of the PaperCut MF Admin web interface.

7. Log in to the device as the simple test user:

8. Verify that the print jobs for the simple test user are being held and listed:

9. To release one or many held print jobs at once, select all the relevant held print jobs and click **Print**.

10. To delete one or many held print jobs at once, select all the relevant held print jobs and click the **Bin** icon.

11. To view and take actions on a single held print job, click the chevron:

Details of the held print job are displayed:

12. Log out of the device.
13. Log in to the PaperCut MF Admin web interface.
14. Navigate to **Logs**.
15. After printing is completed, verify that **Job Log** page displays the test user's name, simple test user, in the **User** column and the **Charged To** column:

16. Log out of the PaperCut MF Admin web interface.

3.2.3 Simple copying

Simple copying does not involve providing the simple test user with a choice of accounts to choose from. Copying is charged to the simple test user's default My Personal Account.
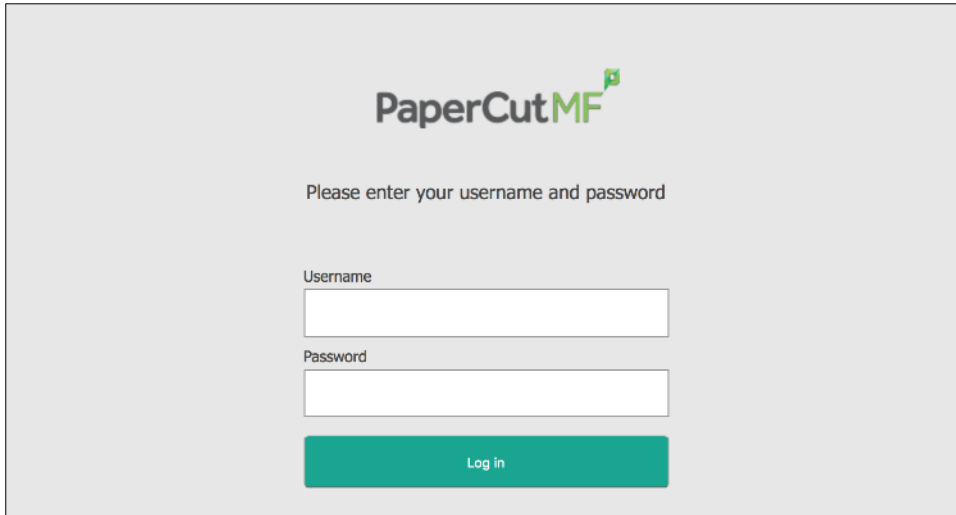
To test simple copying, ensure the following test preparation requirements are met:

- **Simple test user** - A simple test user is created and configured. For more information, see 3.1 Test preparation: create test users and 3.2.1 Test preparation: configure simple test user.
- **Device functions** – Copying is enabled. To enable copying:
    1. Log in to the PaperCut MF Admin web interface.

2. Navigate to **Devices**.

3. Select the device being tested.

4. In the **External Device Settings > Tracking** area, select **Track & control copying.**

5. Click **Apply**.

6. Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.
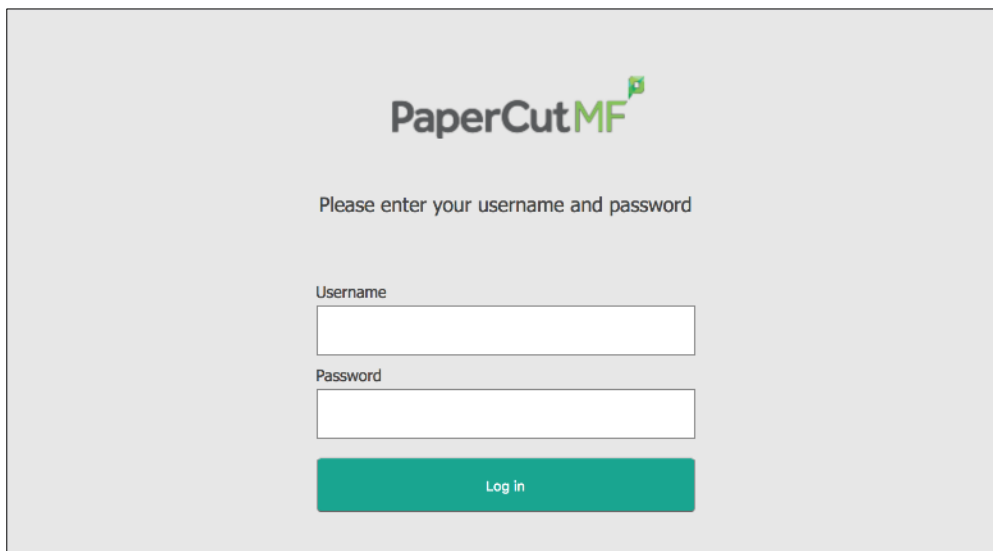
To test simple copying:

1. Log in to the device as the simple test user:

2. Verify that the PaperCut MF Account Confirmation screen does not provide the simple test user with a choice of accounts to choose from, and charges copying to the simple test user's default My Personal Account:

3. Click **Access Device.**

4. Select **Copy**.

5. Complete copying by following the device's workflow.

6. Log out of the device.

7. Log in to the PaperCut MF Admin web interface.

8. Navigate to **Logs**.

9. After copying is completed, verify that **Job Log** page displays the test user's name, simple test user, in the **User** column and the **Charged To** column:

10. Log out of the PaperCut MF Admin web interface.

3.3 Advanced copying

Advanced copying involves providing the advanced test user with a choice of accounts to choose from. Copying is charged to the account that is selected by the advanced test user.

To test advanced copying, ensure the following test preparation requirements are met:

- **Advanced test user** – An advanced test user must be created. For more information, see 3.1 Test preparation: create test users.

  Once created, the advanced test user must be configured.

  To configure the advanced test user:

  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Users**.
  3. From the **User List**, select the advanced test user.
  4. In the **Account Details** area, set the **Balance** to **$50.00** and select **Restricted:**

5. In the **Account Selection** area's **Print account selection**, select **Show standard account selection** and select the relevant option:
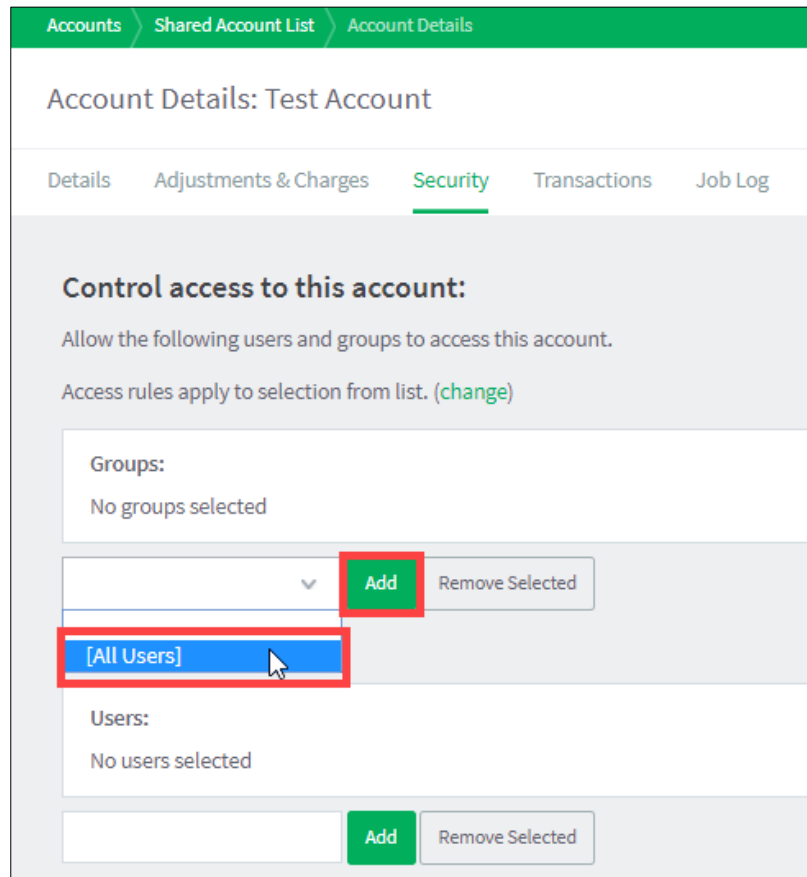
6. Click Apply.

- **Device functions** – Copying is enabled. To enable copying:
    1. Log in to the PaperCut MF Admin web interface.
    2. Navigate to **Devices**.
    3. Select the device being tested.
    4. In the **External Device Settings > Tracking** area, select **Track & control copying.**
    5. Click **Apply**.
    6. Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.

- **Advanced account** – A test account is created.

    To create a test account:
    1. Log in to the PaperCut MF Admin web interface.
    2. Navigate to **Accounts**.
    3. Click **Create a new account…**.
    4. In the **Details & Balance** area's field **Account Name**, enter the name of the test account (test account).
    5. Click **Apply**.
    6. Verify that the **Accounts > Shared Account List** page displays the test account created.
    7. Click the test account.
    8. Navigate to **Security**.
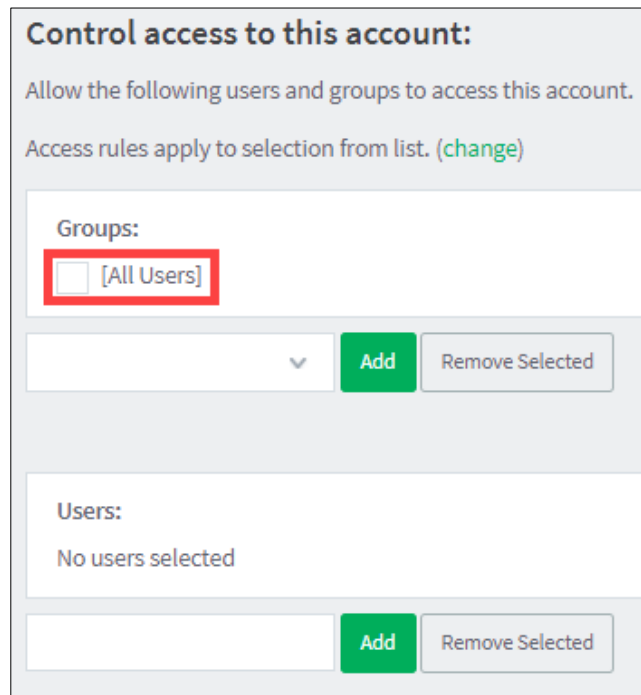
9. In the **Control access to this account > Groups** area, select **[All Users]**; then click **Add**:

10. Verify that the **Control access to this account > Groups** area displays **[All Users]**:
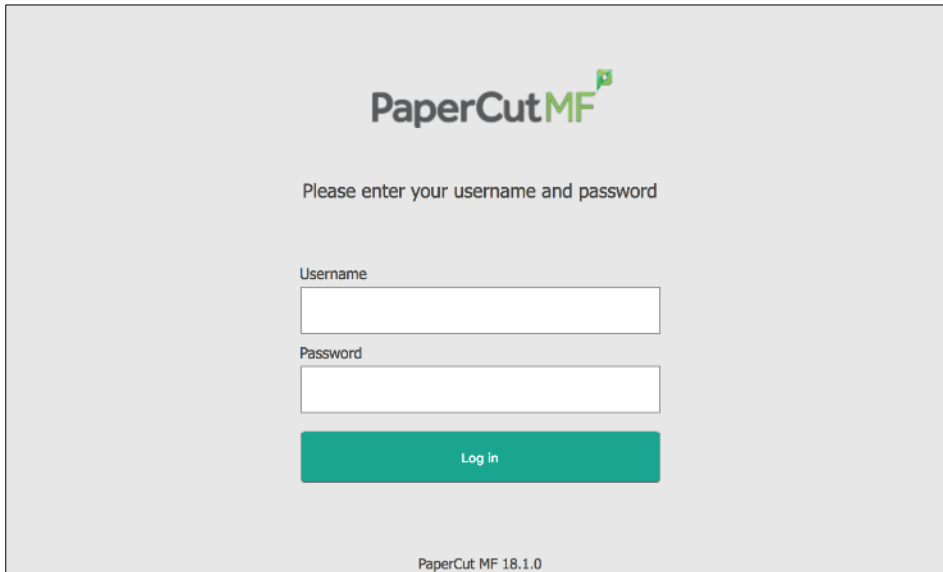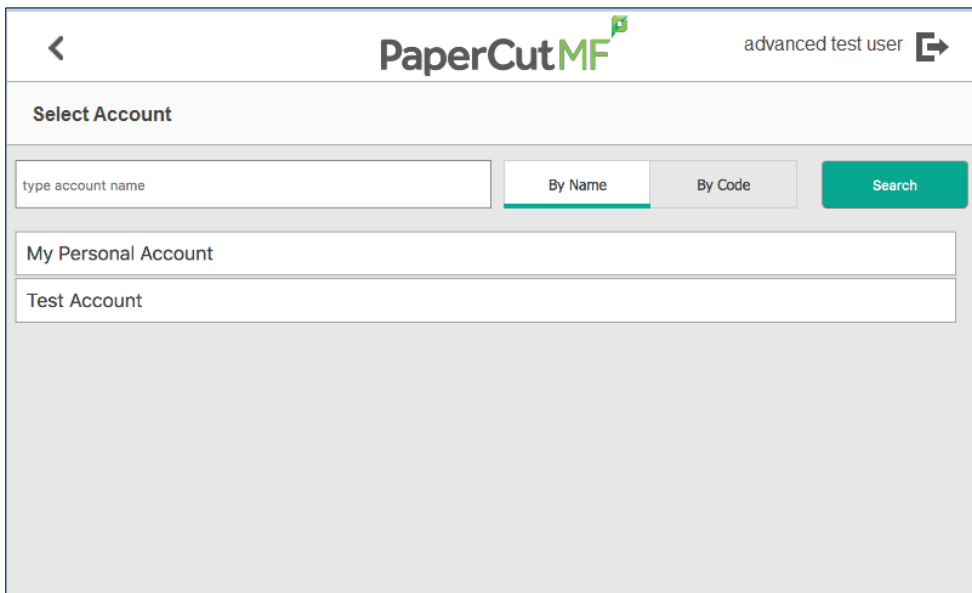
To test advanced copying:

1. Log in to the device as the advanced test user:
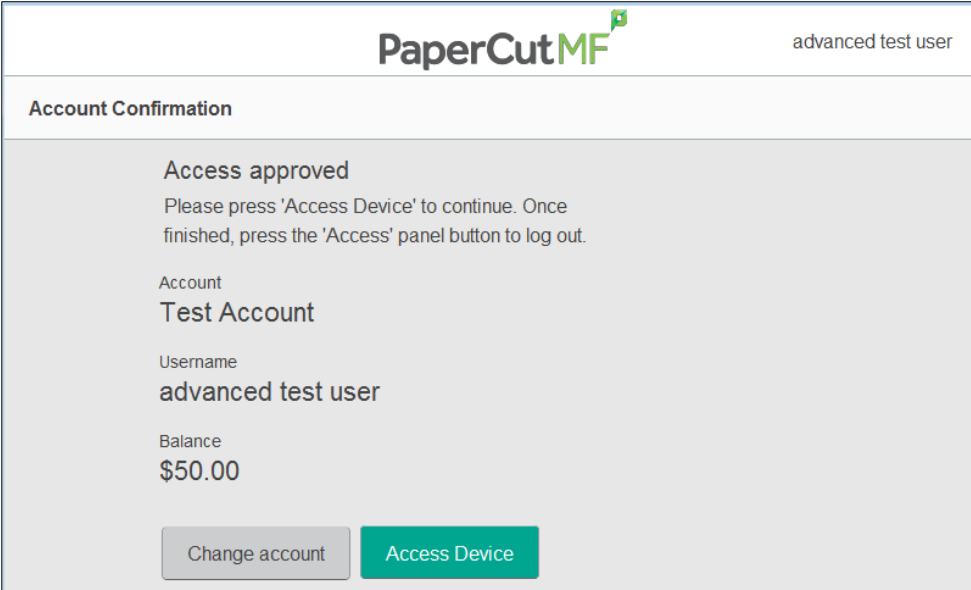
2. Verify that the PaperCut MF Select Account screen provides the advanced test user with a choice of accounts to choose from:

3. Select the relevant account, test account.
4. Verify that the PaperCut MF Account Confirmation screen displays the selected account, test account, but continues to provide the advanced test user with the option of changing the account:
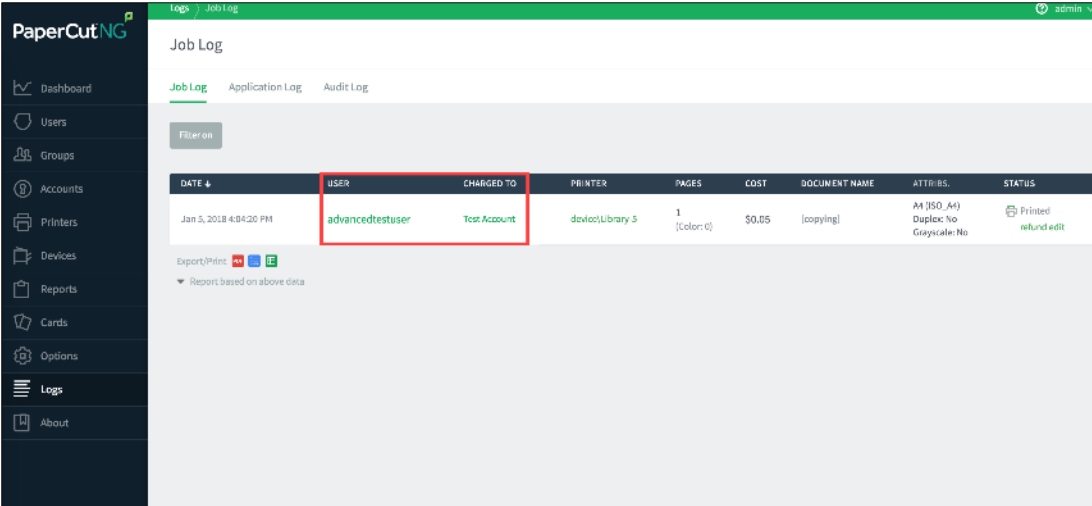
5. Click **Access Device.**

   Copying is charged to the account selected by the advanced test user, test account.

6. Select **Copy**.

7. Complete copying by following the device's workflow.

8. Log out of the device.

9. Log in to the PaperCut MF Admin web interface.

10. Navigate to **Logs**.

11. After copying is completed, verify that **Job Log** page displays the test user's name, advanced test user, in the **User** column and the selected account's name, test account, in the **Charged To** column:

12. Log out of the PaperCut MF Admin web interface.

4 Configuration

PaperCut MF is installed on the device with default settings, which are reasonable for most environments. However, these settings can be further tweaked to suit your environment.

4.1 Inbound connections

4.1.1 Inbound connections to PaperCut MF Application Server

To configure PaperCut MF to allow inbound connections from the device to the PaperCut MF Application Server, use the config key **system.network-address**. For more information, see 4.10 Config Editor.

4.1.2 Inbound connections to PaperCut MF Site Servers

To configure PaperCut MF to allow inbound connections from the device to PaperCut MF Site Servers on the PaperCut MF Admin web interface:

1. Site Servers must already be installed and configured. For more information, see the PaperCut MF manual.
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Sites**.
4. Select the Site Server.
5. In the **Configuration** area, enter the IP address or DNS name of the PaperCut MF Site Server that the device uses to make inbound connections.
6. Click **Apply**.

4.2 Security settings

4.2.1 HTTPS Security (recommended)

PaperCut MF can be configured to communicate with the device using the HTTPS (SSL/TLS) protocol, which is a more secure and encrypted protocol.

To enable HTTPS, you must have an SSL certificate installed on the PaperCut MF Application Server. The certificate must use the server's fully-qualified domain name. This must be defined either in the **Common Name** (CN) field or included in the **Alternative Names** (AN) of the subject of the certificate. Without this, the device cannot connect to the server, since devices do not work with hostname-only certificates (i.e. not fully qualified). Additionally, a complete certificate must contain the following fields: **Version, Serial Number, Signature Algorithm, Signature hash algorithm, Issuer, Valid from/to, Subject, Public Key, Public key Parameters, Authority Key Identifier, Basic Constraints, Key Usage, Subject Alternative Name, Subject Key Identifier, Thumbprint** for the MFP to match the certificate to the device. The **Issuer** and **Subject** fields should include these values: **Country (C)**, **State or Province (S)**, **Locality (L)** and **Organization (O)**.

You may use an official Certificate Authority-signed certificate or a self-signed certificate.

To generate a self-signed certificate with the needed fields, you can follow the steps outlined in 4.2.1.2 Self-signed certificate.

Note: After attempting to enable HTTPS, based on the version of PaperCut MF, the following could apply, resulting in required actions:

- On PaperCut MF 18.3 or above, see 4.2.1.3 SHA 1 warning message on PaperCut MF 18.3 or above
- On PaperCut MF 18.2.6 or below, see 4.2.1.4 SHA 1 warning message on PaperCut MF 18.2.6 or below

4.2.1.1 Certificate Authority (CA) signed certificate

If you are using an official CA-signed certificate (for example, Verisign, Thawte), it is likely to use the server's fully qualified domain name (or wildcard). This is because Certificate Authorities generally no longer accept certificate requests for either intranet names or IP addresses.

4.2.1.2 Self-signed certificate

If you are using the self-signed certificate that is generated by default when installing PaperCut MF, you need to regenerate the certificate to have all the required fields.

If you do not have a certificate set up, follow our guide on creating a keystore, creating a CSR file here: https://www.papercut.com/kb/Main/SSLWithKeystoreExplorer.

Self-signing CSR files:

You can opt to self-sign the generated CSR in the step above.

Here is an example of how to self-sign the CSR file using the OpenSSL tool:

If you do not have OpenSSL, it can be downloaded here: https://www.openssl.org/ or https://wiki.openssl.org/index.php/Binaries

Replace <YOUR CSR FILENAME>, <hostname.domain>, <hostname>, <IP address> with actual values.

openssl genrsa -out rootCA.key 2048

openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.crt

openssl x509 -req -in <YOUR CSR FILENAME>.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out cert.crt -days 825 -sha256 -extfile certificate.ext

where certificate.ext is a file that contains this:

authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:FALSE

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment

subjectAltName = @alt_names

[alt_names]

DNS.1 = <hostname.domain>

DNS.2 = <hostname>

IP.1 = <IP address>

 Make sure to input your self-signed crt file and follow the steps in "Configure PaperCut to use the new keystore" after you have imported your certificate, including updating server.properties file with your keystore information and restarting the PaperCut MF server.

Configure PaperCut MF to use the server's hostname.

1. Log in to MF and navigate **to Options → Config editor (Advanced).**
2. Search for "**system.network-address**". For more information, see **4.10 Config Editor**.
3. Specify the FQDN for the server as the network address. Ensure it is the same address that is used in the certificate and that you can reach the MF server on this name.
4. Restart PaperCut MF to ensure that the changes are applied.

Your device need to be rebooted after PaperCut MF is installed on the device for the new certificate to apply.

4.2.1.3   SHA 1 warning message on PaperCut MF 18.3 or above

If the following warning message is displayed, it implies that the device is using the SHA1 default PaperCut MF certificate:

- PaperCut MF Admin web interface (Devices > External Device List > Device Details):
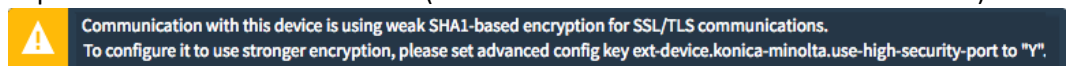
- device:
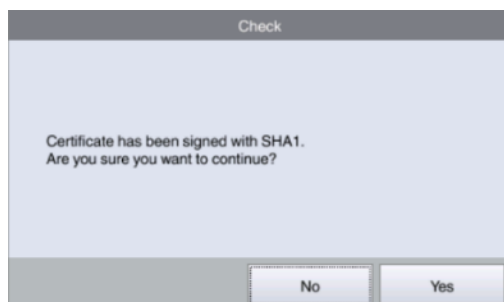
To temporarily resolve it by hiding the message on the:

- PaperCut MF Admin web interface, use the config key **ext-device.konica-minolta.browser.show-sha1-message**. For more information, see 4.10 Config Editor.
- device, users must click **Yes**:
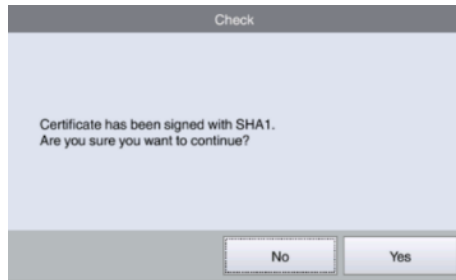
To permanently resolve it, set the config key **ext-device.konica-minolta.use-high-security-port** to **Y** to resolve this. For more information, see 4.10 Config Editor.

4.2.1.4 SHA 1 warning message on PaperCut MF 18.2.6 or below

If the following warning message is displayed, it implies that the device is running the G00-Q1 firmware and is using the SHA1 default PaperCut MF certificate:

- On the PaperCut MF Admin web interface (Devices > External Device List > Device Details):
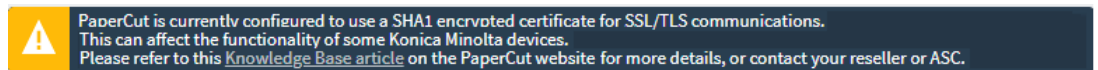
- On the device:
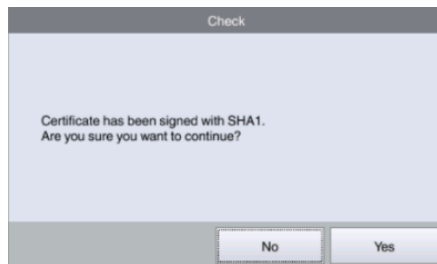
To temporarily resolve it by hiding the message on the:

- PaperCut MF Admin web interface, use the config key **ext-device.konica-minolta.browser.show-sha1-message**. For more information, see 4.10 Config Editor.
- device, users must click **Yes**:

To permanently resolve it:

- see SHA1 error message on Konica Minolta, or
- upgrade to PaperCut MF 18.3.0, or
- contact your Reseller or Authorized Solution Center.

4.2.1.5 Certificate registration warnings

If the device warns that the certificate security credentials could not be verified, this could be due to:

- The certificate that your app server is using has incomplete information.
- The device time is not set. Ensure the device time is set and within the validity of the certificate by logging into the device web interface.

Follow the steps in section 4.2.1 HTTPS Security (recommended) to ensure that your certificate contains complete information. Refer to 4.2.1.1 Certificate Authority signed certificate if using a CA-signed certificate. If using a self-signed certificate, go to 4.2.1.2 Self-signed certificate.

Once you have completed the steps outlined in the sub-section specific to your certificate and the PaperCut MF server has restarted, the newly-generated certificate will be automatically updated onto the device. If you find that the error is still present even after a device reboot, this is because there may be conflicting certificates on the device. Remove the old certificate by logging into the device web interface as an admin.

To do this, navigate to **Security->PKI Settings->External Certificate Setting**. Under **"Trusted CA Root Certificate"**, you may find more than one certificate for your PaperCut MF server. Select the old certificate and delete it. Log out as an admin and reboot the device. After this is completed, the warning should be resolved.

4.2.2 Additional network security

By default, the PaperCut MF Application Server allows device connections from any network address. However, communication between the PaperCut MF Application Server and the device can be further restricted to a set range of network addresses. This provides an additional level of security and ensures that only approved devices are connected to the PaperCut MF Application Server.

To restrict communication between the PaperCut MF Application Server and the device to a subset of IP addresses or subnets on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **Security** area's field **Allowed device IP addresses**, enter a comma-separated list of device IP addresses or subnets (<ip-address1 or subnet-mask1>, <ip-address2 or subnet-mask2>).
4. Click **Apply**.
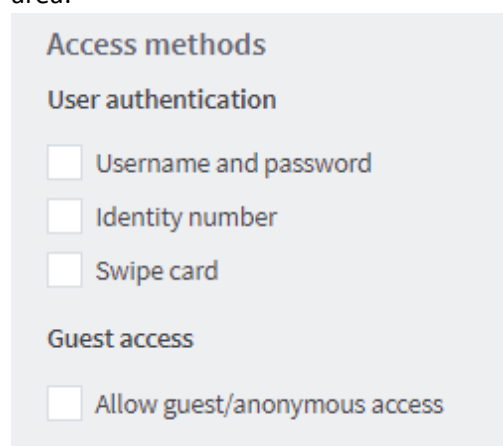
4.3 User authentication options

PaperCut MF provides you with several authentication options to authenticate users when logging in to PaperCut MF on the device.

To configure the device's user authentication:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the relevant device.
   The available authenticate options are in the **Device Details** page's **External Device Settings** area:

   Note: You may use any one or a combination of all the available authentication options, including the guest and anonymous access authentication options.

The available user authentication options are:

User authentication option	Description
Username and password	This is the default authentication option.
	With this option, users use their domain/network username and password.
Identity number	With this option, users use their ID number. For more information, see the [PaperCut MF manual](link).

- **Require PIN:** With this option, users use their id number and the PIN associated with the id number.
  Note: Users can use an id number with or without a pre-set and associated PIN. If using an id number without a pre-set and associated PIN, users are prompted to set a valid PIN to associate with the id number.

Swipe card	With this option, users use their registered swipe card (e.g. magnetic strip, smart card, RFID). For more information, see the [PaperCut MF manual](#). **Note:** If you select this option, then see 4.4 User authentication via swipe cards. • **Require PIN:** With this option, users use their registered swipe card and the PIN associated with the card. **Note:** Users can use a swipe card with or without a pre-set and associated PIN. If using a swipe card without a pre-set and associated PIN, users are prompted to set a valid PIN to associate with the swipe card. • **Enable self-association with existing user accounts**: With this option, users can use a registered swipe card or a new, unregistered swipe card. If using new, unregistered swipe cards, users are prompted to complete card self-association using their username and password (i.e. associating a new unregistered card with a relevant, valid user account). After card self-association is completed, subsequent use of the registered swipe card does not require users to enter their credentials. You may use the config keys: **ext-device.card-self-association.use-secondary-card-number** and **ext-device.self-association-allowed-card-regex.** For more information, see 4.10 Config Editor.
Allow guest/anonymous access	With this option, you may choose to activate **guest** or **anonymous access**, enabling users to be authenticated as guest or anonymous users, as per the user specified in the **Inherit settings from user** field. • **Inherit settings from user:** Enter the username of the PaperCut MF user's profile that is used while authenticating users as guest or anonymous users on the device. • **Guest access** - Selecting the **Allow guest/anonymous access** authentication option *and also* selecting one or more of the other authentication options (Username and

password, Identity number, Swipe card), activates **Guest access**. With this option:

- o A **Guest** button, which may be customized, is displayed on the PaperCut MF Login screen on the device, together with the other authentication options selected.

  Note: To customize the text of the **Guest** button that appears on the PaperCut MF Login screen, use the config key **ext-device.konica-minolta.guest-access.label.** For more information, see 4.10 Config Editor.

- o A user clicking this **Guest** button is authenticated as a guest user, as per the user specified in the **Inherit settings from user** field.

- **Anonymous access** - Only selecting the **Allow guest/anonymous access** authentication option *without* selecting any other authentication option, activates **Anonymous access**. With this option:

  - o A user is authenticated as an anonymous user, as per the user specified in the **Inherit settings from user** field.
  - o This anonymous user can view held print jobs belonging to all users.

4.4 User authentication via swipe cards

4.4.1 Supported card readers

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

1. AU-201 (MIFARE/Type-A cards)
2. HID Omnikey CardMan 5125 (HID Proximity cards)
3. AU-202H (HID iClass cards)
4. AU-204H Magtek (Magstripe cards)
5. AU-205H / HID Omnikey 5427CK (HID Proximity/MIFARE/Type-A cards)
6. RF Ideas 6381AK0 (Indala), RDR-7581AK0 (Mifare)
7. 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.

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 support at the firmware level, as new devices become available. 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.

4.4.2   Handling card identifiers

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

- Cards whose identifiers consist of a number followed by a 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 options:

- 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 options 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**.

4.4.2.1   Regular expression filters

To extract and validate card identifiers using regular expression filters, use the config keys **ext-device.card-no-regex**, **ext-device.self-association-allowed-card-regex**.

Note: If you customize BOTH the config **keys ext-device.card-no-regex** and **ext-device.self-association-allowed-card-regex**, then you must ensure that:

- **ext-device.card-no-regex** is the extraction pattern (i.e. the "full regular expression filter" based on which card identifiers are extracted)
- **ext-device.self-association-allowed-card-regex** is the validation pattern (i.e. validates only the "truncated part of the card identifier" that was extracted by the extraction pattern of ext-device.card-no-regex)

For example:

if, ext-device.card-no-regex = \d{6}(\d{8})

then, ext-device.self-association-allowed-card-regex = \d{8}

For more information, see 4.10 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.

4.4.2.2 Standard format converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see 4.10 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.	

4.4.2.3 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 4.10 Config Editor.

4.5 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 4.10).

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 4.10).

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.

4.6 Secure print release

Secure Print Release causes all print jobs to be held at the device until a user releases the job. If the device is configured with Secure Print Release, then when releasing held print jobs, users can select the following:

- the account

- [the job attributes](#)

To configure Secure Print Release:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the relevant device.
4. In the **Print Release** area, select **Enable print release**.
5. In the **This device will display jobs for release from the selected source queues**, select the relevant Hold/Release queue. For more information, see the [PaperCut MF manual](#).
6. If using PaperCut MF 18.1.4 or below, select **Show button to release all pending jobs** to display the **Print All** button on the PaperCut MF Print Release screen on the device.
   For more information, see 5.5 The "Print All" button on the PaperCut MF screens on the device.

4.6.1 User selection of an account

All print jobs must be allocated to an account before they can be released (printed). This account can be either:

- a user's personal account, or
- a shared account for cost center, faculty, or client billing purposes.

Users can allocate an account to a print job via the User Client and/or at the device. For more information about configuring cost allocation for users, see the [PaperCut MF manual](#).

At the device, users can:

- allocate the same account to *multiple* held print jobs without an account:

- allocate an account to a *single* held print job without an account or change a previously allocated account:
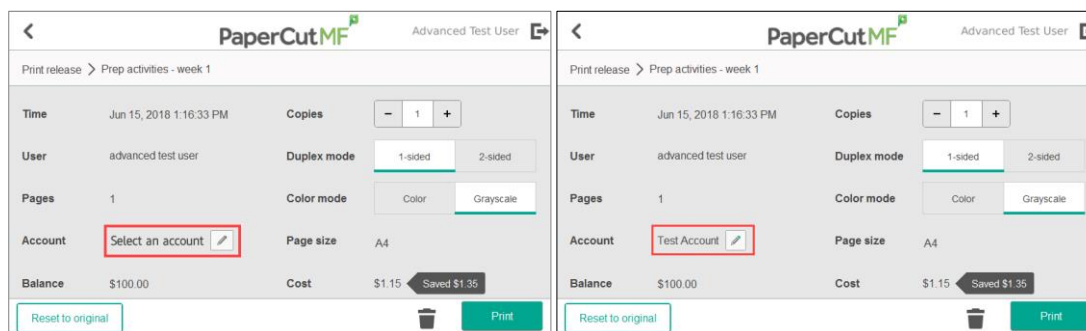
Note: By default, PaperCut MF allows users to select accounts at the device. However, you also have the option of disabling this. For more information, see the [PaperCut MF manual.](#)

4.6.2 User selection of job attributes

PaperCut MF allows users to change the attributes of held print jobs at the device, before releasing (printing) them. Based on the changes made, PaperCut MF shows the updated cost and savings, to give immediate positive feedback to the user, encouraging behavior change.

Users can make the following changes to one or many jobs, simultaneously:

- **Print as grayscale** (from color to grayscale)
- **Print as 2-sided** (from 1-sided to 2-sided)
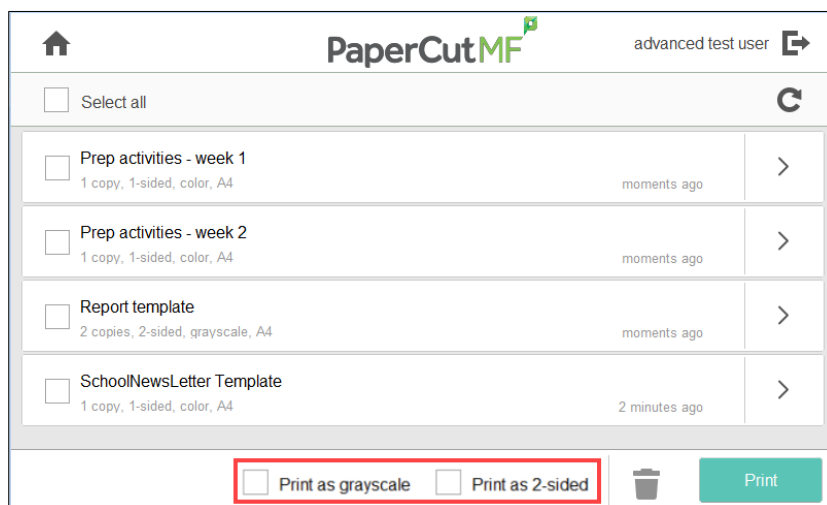
Clicking the arrow to the right of a single held print job displays all the attributes for that job, allowing users to make the following additional changes:

- **Copies**
- **Duplex mode** (from 1-sided to 2-sided)
- **Color mode** (from color to grayscale)
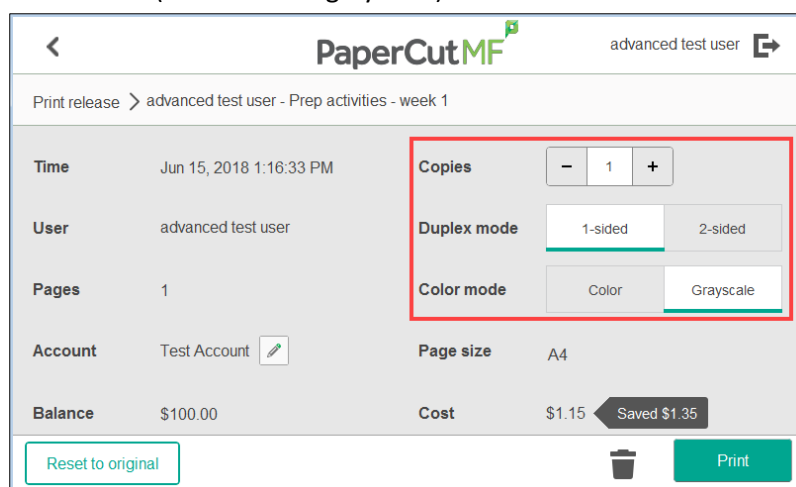
To toggle the display of the cost of held print jobs on the PaperCut MF Print Release and Print Settings screens on the device, use the config key **ext-device.konica-minolta.release.show-cost**. For more information, see 4.10 Config Editor.

Note: By default, PaperCut MF allows users to select jobs attributes at the device. However, you also have the option of disabling this. For more information, see the [PaperCut MF manual.](#)

4.7 Device jobs

Device jobs include jobs initiated at the device, such as, scan, copy, fax, on-device printing.

4.7.1 Tracking device jobs

To specify the device jobs that PaperCut MF tracks and controls:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the relevant device.
4. In the **External Device Settings** area, select the relevant device jobs:
   - **Track & control copying** – PaperCut MF tracks and controls copy jobs and on-device print jobs
   - **Track & control scanning** – PaperCut MF tracks and controls scan jobs
   - **Track & control faxing** – PaperCut MF tracks and controls fax jobs

4.7.2 User selection of an account

If tracked device jobs (scan, copy, fax, on-device printing) are also being charged, then users must

allocate them to an account.

This account can be either:

- a user's personal account, or
- a shared account for cost center, faculty, or client billing purposes.

The options available to users at the device, is based on the way users and the device are configured:

- For more information about configuring cost allocation for users, see the [PaperCut MF manual](#).
- To toggle the display of the PaperCut MF Account Confirmation screen, use the **Show account confirmation** checkbox on the PaperCut MF Admin web interface (**Devices Details > Summary > External Device Settings > Device Options**).
- To configure the PaperCut MF Select Account screen, use the config **ext-device.konica-minolta.accounts.initial-tab.** For more information, see 4.10 Config Editor.

4.7.3 PaperCut MF's Integrated Scanning

To enable users to use PaperCut MF's Integrated Scanning:

1. Configure Integrated Scanning on the PaperCut MF Admin web interface. For more information, see Integrated Scanning or the [PaperCut MF manual.](#)
2. Depending on the needs of your environment, you may need to change the default settings of the following config keys:
   - **ext-device.konica-minolta.custom-my-panel**
   - **ext-device.konica-minolta.auth.public-setting**
   - **ext-device.konica-minolta.device-type-a4**

- **ext-device.konica-minolta.allow-third-party-scan-apps**
- **ext-device.konica-minolta.browser.scanning-compact-pdf**
- **ext-device.konica-minolta.scan.prompt.checkbox.checked**
- **ext-device.konica-minolta.scan.additional-pages.checkbox.checked**
- **ext-device.konica-minolta.browser.scanning-merge-pdf**
- **ext-device.konica-minolta.browser.scanning-merge-tiff**
- **ext-device.konica-minolta.timeout.scan-prompt-send.secs**

For more information, see 4.10 Config Editor.

4.7.3.1 Integrated scan workflow

If Integrated Scanning is enabled, then you can use the config key **ext-device.konica-minolta.scan.prompt.checkbox.checked** to specify whether the **New document** checkbox on the Scan Details screen and the Scan Settings screen, is checked or unchecked by default (See 4.10 Config Editor).

- A checked **New document** checkbox enables the device to display the PaperCut MF Scan Complete (with the two buttons - **New Scan Document**, **Send**) screen, providing users with the ability to carry out multiple scan jobs with the same scan settings as the first scan job:
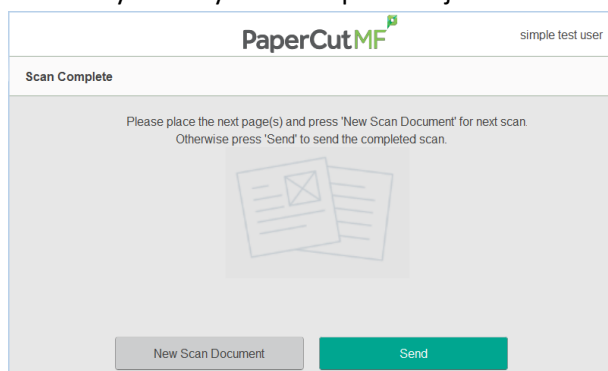
    Note: To specify the user inactivity timeout on this screen, use the config key **ext-device.konica-minolta.timeout.scan-prompt-send.secs**. For more information, see 4.10 Config Editor.

- An unchecked **New Scan Document** checkbox enables the device to complete the current scan and send it to the user (scan transfer).

The configuration that is required to allow users to load pages in batches and receive the entire scan job as a single PDF, is based on the device's i-Option OpenAPI version. After which, PaperCut MF's Integrated Scanning workflow works with the device's scanning workflow as follows:

- **On devices that support i-Option OpenAPI 4.9 or higher**:
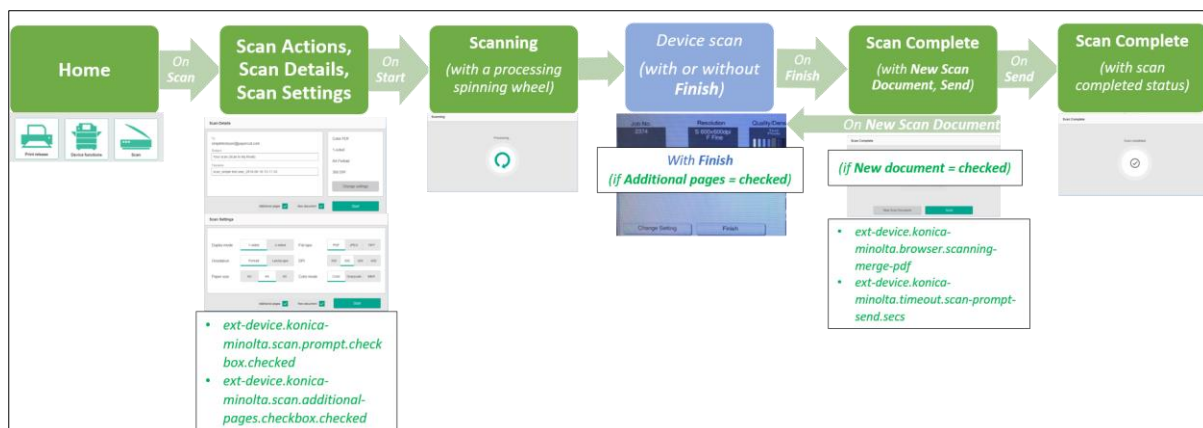
Ensure the config key **ext-device.konica-minolta.scan.additional-pages.checkbox.checked** is set to **Y**. This displays the **Finish** button on the device's scanning screen, allowing users to add more pages to a current PDF scan job and receive it as a single PDF:
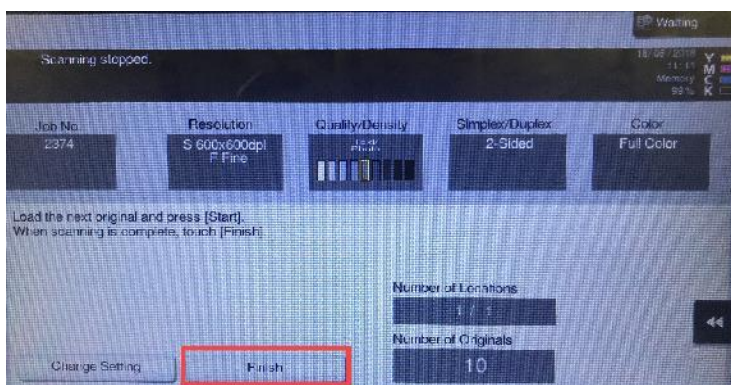
- **On devices that support i-Option OpenAPI 4.8 or lower:**
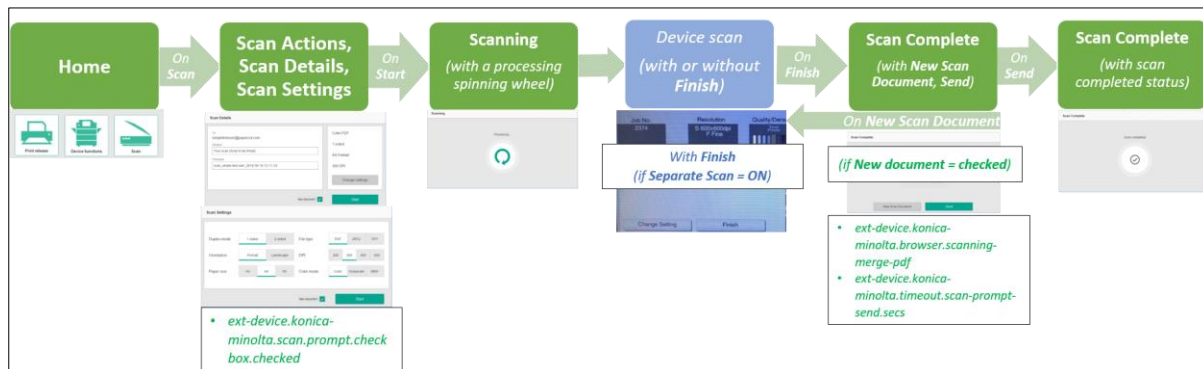
Ensure the device's **Separate Scan** setting is set to **On**. This displays the **Finish** button on the device's scanning screen, allowing users to add more pages to a current PDF scan job and receive it as a single PDF.

To set the device's **Separate Scan** settings:

1. Log in to the device.
2. Navigate to: **Device functions** > **Scan/Fax > Application**
3. Toggle **Separate Scan** to set it to **On**:

4. Navigate to **Menu** > **Utilities** > **User Settings** > **Scan/Fax Settings**.
5. Set the **Default Scan/Fax Settings** field to **Current Setting**.
   Note: If the **Default Scan/Fax Settings** field is already set to **Current Setting**, then first set it to **Default Setting**, and then set it to **Current Setting.**
6. Click **Ok**.
7. Click **Close**.

4.8 PaperCut MF's Language Selection

PaperCut MF allows authenticated users to select their preferred language at the device. After a user has selected a language, that language is used when they log in to any device that supports language selection at any location. This is particularly useful in multilingual and bilingual countries, such as Canada, Singapore, and India and for the *set-and-forget convenience.*

Note: The language selected at the device:

- does not persist for **Guest or anonymous** logins
- does not change the device's currency and paper size values to correspond to the geographical locale of the changed language. For example, if the device is installed in Canada, and a user changes the device's language to French, then the currency does not automatically change to Euros.

To configure PaperCut MF's Language Selection:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the relevant device.
4. In the **Device Language Settings** area, select either:
   - **Use device default language**—users cannot select their preferred language via PaperCut MF's Language Selection. The language used is the value of the config key **ext-device.konica-minolta.locale**
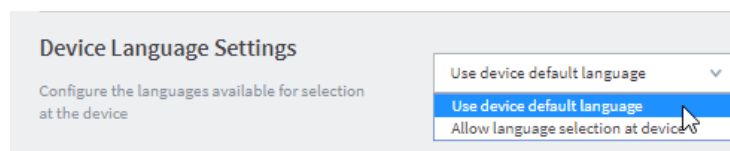
- **Allow language selection at device**— allow users to select their preferred language via PaperCut MF's Language Selection.
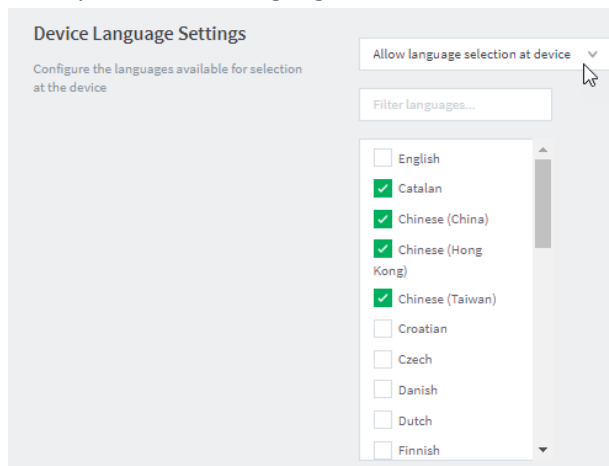
4. If you selected **Allow language selection at device**, select the languages you want to make available for users.
5. Click **OK**.

After configuring PaperCut MF's Language Selection, check that it works at the device:

1. Tap the globe button with the 3-letter language code to display the list of available languages.
   Note: The language code is determined by the value of the config key **ext-device.konica-minolta.locale**
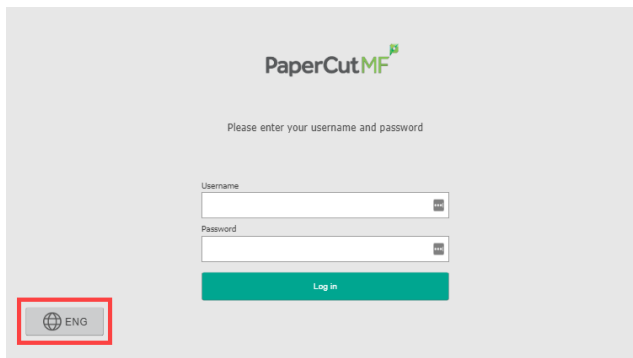
2. Select a language.
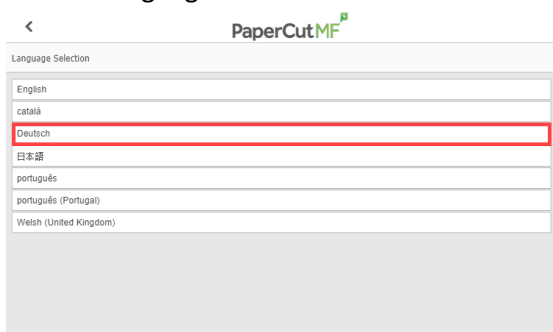
The PaperCut MF Login screen is displayed with the 3-letter language code for the selected language.

3. Log in to the device as a test user.

   The text on all the PaperCut MF screens is displayed in the selected language:
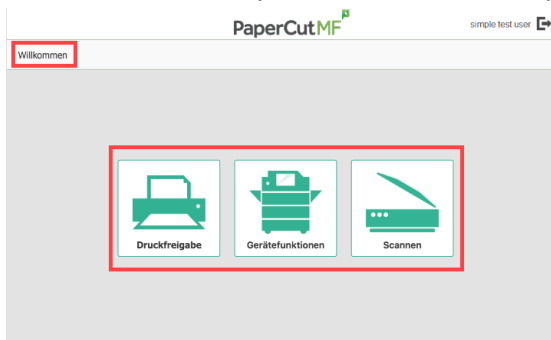
4. Log out of the device.

   The globe button's 3-letter language code reverts to the device's default language ready for the next user.
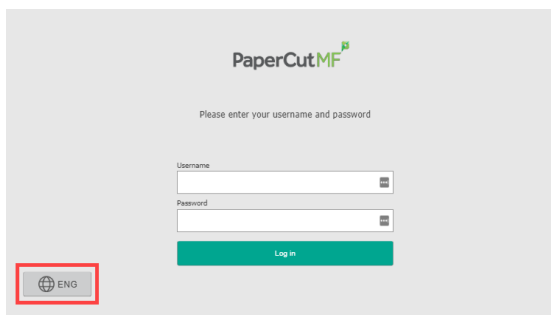
5. Log in to the device as the same test user.

   Check that the text on all the PaperCut MF screens is displayed in the previously selected language:

4.9 Screen headers

4.9.1   Header colors

To customize the colors of the background, text, and buttons of the headers on all PaperCut MF screens:

1.   Use the following config keys:

     ext-device.konica-minolta.browser.header-color
     ext-device.konica-minolta.browser.header-text-color
     ext-device.konica-minolta.browser.header-image-color
     For more information, see 4.10 Config Editor.
2.   Log in to the device as a test user (simple test user).
3.   Verify that the colors of the background, text, and buttons of the headers on all PaperCut MF screens are as required.

4.9.2   Header logo

To customize the logo on the headers of all PaperCut MF screens:

1.   Create the device's header logo as per the following specifications:
     - Image height = 50 pixels
     - Image width = 260 pixels
     - Image file format = `.png`
     - Image filename = `logo.png`
     - Image file location = `[PaperCut Install Location]\server\custom\web\device\konica\ioption\`
2.   Log in to the device as a test user (simple test user).
3.   Verify that the device's header logo is as required.

4.10 Config Editor

PaperCut MF provides you with several global and device-specific config keys that you can modify to suit your environment. While some keys are *only* global (impacting PaperCut MF on all devices) or *only* device-specific (impacting PaperCut MF on the selected device), other keys are *both* global *and* device-specific simultaneously. Such keys initially inherit their global settings (GLOBAL) as their default settings. However, changes made at the device-level overrides these globally inherited default settings.

To access the available global config keys (impact PaperCut MF on all devices) on the PaperCut MF Admin web interface:

1.   Log in to the PaperCut MF Admin web interface.
2.   Navigate to **Options > Actions > Config editor (advanced).**
     Note: For more information, see the PaperCut MF manual.

To access the available device-specific config keys (impact PaperCut MF on the selected device) on the PaperCut MF Admin web interface:

1.   Log in to the PaperCut MF Admin web interface.
2.   Navigate to **Devices.**

3. Select the device.
4. Click **Advanced Config.**

The available config keys are:

Config name	Description
Device screens	
ext-device.konica-minolta.locale	Specify the default language of the device, if it is different to the language of the locale in which the device was installed. This is a device-specific config key. - Values: xx (language), xx_XX (language_region), DEFAULT For example, ja (Japanese), en_US (English_United States of America) - Default: DEFAULT (language of the locale in which the device was installed) **Note:** - Changing this config key's default value does not change the device's currency and paper size values to correspond to the geographical locale of config key's value. For example, if the device is installed in Canada, and this config key's value is French, the device's currency does not change to Euros. It remains Canadian Dollar. - This config key's value is overridden when a user changes the device's language using the configured PaperCut MF Language Selection. For more information, see 4.8 PaperCut MF's Language Selection.
ext-device.konica-minolta.browser.header-color	Customize the background color of headers on all PaperCut MF screens. This is a device-specific config key. - Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT - Default: DEFAULT (white) **Note:** For more information, see 4.9.1 Header colors.

ext-device.konica-minolta.browser.header-text-color	Customize the text color of headers on all PaperCut MF screens. This is a device-specific config key. • Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT (dark grey) **Note:** For more information, see 4.9.1 Header colors.
ext-device.konica-minolta.browser.header-image-color	Customize the color of the buttons (**Home** icon, **Logout** icon, **Back** chevron icon, **Access Device** button) on the headers of all PaperCut MF screens. This is a device-specific config key. • Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT (#555555, dark grey) **Note:** For more information, see 4.9.1 Header colors
ext-device.konica-minolta.browser.screen-height	Overrides the auto detected panel resolution/screen height. When set to a positive integer, the value represents the screen height in pixels. Default: 0 (auto)
ext-device.konica-minolta.browser.screen-width	Overrides the auto detected panel resolution/screen width. When set to a positive integer, the value represents the screen width in pixels. Default: 0 (auto)
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.login.enable-auto-submit	Configure the PaperCut login behavior that is most suitable to the type of keyboard you are using – either the soft on-screen keyboard or the external hard keyboard. Values: Y, N Default: Y Setting this to Y is recommended when a soft on-screen keyboard is operational. If an external hard keyboard is operational, then this will result in the login workflow getting auto-submitted for authentication, as soon as a value is entered on a field. Setting this to N is recommended when an external hard keyboard is operational. If a soft on-screen keyboard is operational, then this will require users to press the Ok / Enter / Return button twice on each login step / field (once to minimize the keyboard and a second time to move to the next step / field).

ext-device.konica.browser.chromium.popup-keyboard	Specify the type of soft keyboard used by the device:
	
	• either, partially covering the device's screen,
	• or, entirely covering the device's screen.
	
	Values = Y (partially covers screen), N (entirely covers screen)
	
	Default = DEFAULT (Y)
	
	Note:
	
	o This is only applicable to Chromium browser devices running the function version 4.2 or above.
	o Setting this to DEFAULT/ Y –
	   o is recommended if the device's soft keyboard partially covers the screen.
	   o is not recommended if the device's soft keyboard entirely covers the screen because it makes some of the text fields on the device unusable.
	o Setting this to N –
	   o is recommended if the device's soft keyboard entirely covers the screen.
	   o is not recommended if the device's soft keyboard partially covers the screen because it stops a user's changes to text

	fields on the Scan Details screen from being saved if this is followed by clicking the device's hard Start key to start a new Integrated Scan job.
ext-device.konica-minolta.auth.screen.title	Customize the name of the PaperCut MF Login screen. This is a device-specific config key.
ext-device.konica-minolta.message.welcome.line1	Customize text that appears on the PaperCut MF Login screen. For example, instructions to help users log in to PaperCut MF on the device.
ext-device.konica-minolta.message.welcome.line2	This is a device-specific config key. • Values: Any text, DEFAULT • Default: DEFAULT (device-specific PaperCut MF text)
ext-device.konica-minolta.guest-access.label	Customize the text of the **Guest** button that appears on the PaperCut MF Login screen. This is a device-specific config key. • Values: Any text, DEFAULT • Default: DEFAULT (Guest) **Note:** This is applicable only if **guest access** is activated (the **Allow guest/anonymous access** authentication option is selected and at least any one other authentication option is also selected). For more information, see 4.3 User authentication options.
ext-device.konica-minolta.login-confirmation-message	Allows for optional text to be configured and presented on the device, as part of the overall login confirmation screen message and instructions.
ext-device.konica-minolta.browser.show-logout-button	Allows logout button to be hidden in the login interface. Users can logout while in the middle of the login workflow by pressing the "reset" key on the device panel instead. Default: Y

ext-device.konica-minolta.enable.screen-logout-button	Display the **Logout** button on all PaperCut screens on the device. Clicking this will log out the user and display the PaperCut login page. Values: Y, N Default: N
ext-device.konica-minolta.browser.show-back-button	If back button is shown in the login interface it can be hidden similarly to ext-device.konica-minolta.browser.show-logout-button. Default: Y
ext-device.konica-minolta.browser.device-function-button.title	Customize the text of the **Device Function** icon that appears on the PaperCut MF Home screen. This is a device-specific config key. • Values: Any text, DEFAULT • Default: DEFAULT (Device Function)
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.custom-my-panel	Displays the Scan and the Release icon on the device panel. Values: Y, N. Default N If you change the value from Y to N, some devices need to be restarted. **Note:** This feature is not supported on C3350, C3850, C3850FS, 4050, and 4750 devices.
ext-device.konica-minolta.app-release.title	Allows customising of the PaperCut's print release application title without also customising 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 customised 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.home-screen.force-show** | Customize whether the PaperCut MF Home screen is made available or not to users. |

This is a global config key.

- Values: N (PaperCut MF Home screen is unavailable), Y (PaperCut MF Home screen is available)
- Default: N

Note:

- Setting this to N – makes the PaperCut MF Home screen unavailable to users only if both the following conditions are also met:
    - **Integrated Scanning** is not selected, and
    - **Enable print release** is not selected

  After successfully logging in to the device from the PaperCut MF Login screen, users are shown the PaperCut MF Select Account screen. However, if both the above conditions are not met, then after successfully logging in to the device from the PaperCut MF Login screen, users are shown the PaperCut MF Home screen. The PaperCut MF Home screen displays any one or all of the following options, based on the other settings:
    - **Device functions**
    - **Scan** (if **Integrated Scanning** is selected)
    - **Print release** (if **Enable print release** is selected)
- Setting this to Y – makes the PaperCut MF Home screen available to users. After successfully logging in to the device from the PaperCut MF Login screen, users are shown the PaperCut MF Home screen. The PaperCut MF Home screen

	displays any one or all of the following options, based on other settings:
	
	  ○ **Device functions**
	  ○ **Scan** (if **Integrated Scanning** is selected)
	  ○ **Print release** (if **Enable print release** is selected)

ext-device.konica-minolta.browser.enable-fast-login-flow	Reduces the login time when all the following conditions are satisfied: • A swipe card is used to login AND • None of the following features are enabled: Account Selection, Account Confirmation, Print Release, Integrated Scanning AND • The global key ext-device.home-screen.force-show global config is set to Default or N. Values = Y, N. Default = DEFAULT (Y) Setting this to Default or Y will reduce swipe-card login time. Setting this to N will extend the swipe-card login time. **Note:** This setting on any of the following devices will make them unusable, unless the ext-device.konica-minolta.device-type-a4 key is set to Y: • bizhub C3850FS, bizhub C3850, bizhub C3350 • bizhub 4050, bizhub 4750
ext-device.konica-minolta.browser.suppress-home-screen	Configure the workflow to suppress the display of the PaperCut MF Home screen after login. Values: Y, N Default: N Setting this to N – does not suppress the PaperCut MF Home screen after login. Any one of the following screens maybe displayed, based on other settings: • The PaperCut Home screen OR • The PaperCut Print Release screen OR • The PaperCut Select Account screen OR • The PaperCut Account Confirmation screen OR • the native device functions screen

	Setting this to Y – suppresses the PaperCut MF Home screen after login. Any one of the following screens maybe displayed, based on other settings: • The PaperCut Select Account screen OR • The PaperCut Account Confirmation screen OR • The PaperCut Print Release screen OR the native device functions screen
ext-device.konica-minolta.login.show-release	Specify whether to include the "Print Release" screen in the login workflow if the device is configured as a release station. Values: Y, N. Default: Y If set to "N", the user must login and press the "Release" button on the device screen to access the release jobs application.
ext-device.konica-minolta.release.show-cost	Toggle the display of the cost of held print jobs on the PaperCut MF Print Release screens. This is a device-specific config key. • Values: Y, N • Default: Y **Note:** Setting this to N also hides the account balance and does not display the savings based on other changes made to held print job settings. For more information, see 4.6.2 User selection of job attributes.
ext-device.konica-minolta.display-balance	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.models-w-optional-username-field	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-minolta.device-type-a4	Specify the orientation mode of PDF Integrated Scan jobs produced by some older compact devices:
	
	• either, based on the user's **Orientation** scan settings (i.e. portrait is scanned as portrait and landscape is scanned as landscape)
	• or, always in landscape.
	
	Values: Y (user-defined), N (always in landscape), DEFAULT
	
	Default: DEFAULT (N)
	
	Note:
	
	• This is only applicable to PDF Integrated Scan jobs. It has no impact on JPEG, TIFF Integrated Scan jobs.
	• Setting this to Y –
	    o is only recommended for some older compact devices (i.e. older devices that do not accept paper sizes higher than Letter or A4).
	    o ensures that the orientation of PDF Integrated Scan jobs produced by these older compact devices is based on the user's **Orientation** scan settings.
	    For more information, see 5.11 Integrated Scans on some devices are always in landscape mode.

ext-device.konica-minolta.browser.scanning-compact-pdf	Specify the PDF format to use when scanning to PDF using Integrated Scanning. **Note:** This is applicable only when Integrated Scanning is enabled. Values: Y (Compact PDF format), N (Uncompressed PDF format) Default: N
ext-device.konica-minolta.email.personalized-sender	Customize the auto-population of a user's email address if using the non-PaperCut MF **Scan-to-Me** on the device. This is a device-specific config key.

- Values: Y, N
- Default: Y

Note: This is applicable only if users' email addresses are already configured while creating and configuring users in PaperCut MF (**Users > User List > User Details > Primary email**).

ext-device.konica-minolta.scan.prompt.checkbox.checked	Specify the default setting of the PaperCut MF Scan screens' **New document** checkbox (checked or unchecked) and the display of the PaperCut MF Scan Complete (with the two buttons - **New Scan Document**, **Send**) screen. This is a device-specific config key. • Values: Y (checked by default; can be changed by the user), N (unchecked by default; can be changed by the user) • Default: Y **Note:** • A checked **New document** checkbox displays the PaperCut MF Scan Complete (with the two buttons - **New Scan Document**, **Send**) screen, providing users with the option of starting a new scan with the current scan's settings. • An unchecked **New document** checkbox hides the PaperCut MF Scan Complete (with the two buttons - **New Scan Document**, **Send**) screen. After the completion of the current scan job, the process of sending it to the user (scan transfer) is automatically initiated. As a result, users are not provided with the option of starting a new scan with the current scan's settings.
ext-device.konica-minolta.scan.additional-pages.checkbox.checked	Specify the default setting of the PaperCut MF Scan screens' **Additional pages** checkbox (checked or unchecked). This is a device-specific config key. • Values: Y (checked by default; can be changed by the user), N (unchecked by default; can be changed by the user)

- Default: Y

Note:

- This only applies to devices that support i-Option OpenAPI 4.9 or higher.
- A checked **Additional pages** checkbox displays the **Finish** button on the device's scanning screen, allowing users to add more pages to a current PDF scan job and receive it as a single PDF.
- An unchecked **Additional pages** checkbox hides the **Finish** button on the device's scanning screen. Users are unable to add more pages to the current PDF scan job and receive it as a single PDF.

ext-device.konica-minolta.browser.scanning-merge-pdf	Specify the impact of the PaperCut MF Scan Complete (with the two buttons – **New Scan Document**, **Send**) screen's **New Scan Document** button on PDF scans. This is a device-specific config key. - Values: Y, N - Default: DEFAULT (N) **Note:** - Setting this to N – does not merge subsequently added pages with a previously completed scan job into one PDF, as one scan job. Every time a user clicks the **New Scan Document** button, a new scan job PDF is created, tracked and sent to the user. - Setting this to Y – merges subsequently added pages with a previously completed scan job into one PDF, as one scan job. However, the PaperCut MF Admin web interface's Job Log lists multiple scan job rows, one for each time the user clicked the **New Scan Document** button. This setting is not recommended if your device is enabled with **Advanced Charging**. For more information, see 5.13 Impact of Advanced Charging on Integrated Scanning.

ext-device.konica-minolta.browser.scanning-merge-tiff	Specify the impact of the PaperCut MF Scan Complete (with the two buttons – **New Scan Document**, **Send**) screen's **New Scan Document** button on TIFF scans. This is a device-specific config key. • Values: Y, N • Default: DEFAULT (N) **Note:** • Setting this to N – does not merge subsequently added pages with a previously completed scan job into one TIFF, as one scan job. Every time a user clicks the **New Scan Document** button, a new scan job TIFF is created, tracked and sent to the user. • Setting this to Y – merges subsequently added pages with a previously completed scan job into one TIFF, as one scan job. However, the PaperCut MF Admin web interface's Job Log lists multiple scan job rows, one for each time the user clicked the **New Scan Document** button. This setting is not recommended if your device is enabled with **Advanced Charging**. For more information, see 5.13 Impact of Advanced Charging on Integrated Scanning.

ext-device.konica-minolta.accounts.initial-tab	Specify the tab that is displayed by default on the PaperCut MF Select Account screen.
	
	This is a device-specific config key.
	
	• Values: Any one of the following tabs:
	    o LIST
	    o SEARCH
	    o CODE
	• Default: LIST
	
	Note: This is applicable only to users configured with the relevant Account Selection options. For more information about configuring cost allocation for users, see the PaperCut MF manual.

"Swipe card" authentication option

ext-device.card-self-association.use-secondary-card-number	Customize the use of the primary or the secondary card number slot to save card identifiers during card self-association. This is a global and device-specific config key. Device-specific: - Values: Y, N, GLOBAL (inherited from global settings) - Default: GLOBAL (inherited from global settings) Global: - Values: N (Primary), Y (Secondary) - Default: N **Note:** This is applicable only if the **Swipe card** - **Enable self-association with existing user accounts** authentication option is selected. For more information, see 4.3 User authentication options.
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: .* **Note:** - This is applicable only if the **Swipe card** - **Enable self-association with existing user accounts** authentication option is selected. For more information, see 4.3 User authentication options and 4.4.2 Handling card identifiers. - Changing the default value of the config key **ext-device.card-no-regex** (extracting card identifiers using customized regular expression filters) requires you to ensure that the value of this config key is only the "truncated part of the card identifier" that was extracted by the extraction pattern of **ext-device.card-no-regex**. For example, if the config key ext-device.card-no-regex = \d{6}(\d{8}), then the config key ext-device.self-association-allowed-card-regex = \d{8}. For more information, see 4.4.2.1 Regular expression filters.

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 option is selected. For more information, see 4.3 User authentication options and 4.4.2 Handling card identifiers.
- Changing the default value of this config key requires you to ensure that the value of the config key **ext-device.self-association-allowed-card-regex** is only the "extracted, truncated part of the card identifier" of this config key. For example, if the config key ext-device.card-no-regex = \d{6}(\d{8}), then the config key ext-device.self-association-allowed-card-regex = \d{8}. For more information, see 4.4.2.1 Regular expression filters.

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 option is selected. For more information, see 4.3 User authentication options and 4.4.2 Handling card identifiers.
ext-device.konica-minolta.card-decoder-hid	Selects the method used to read a user ID from an HID RFID card reader. $0 \rightarrow$ the card number field from OmniKey readers is used as the PaperCut user ID. $1\rightarrow$ 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.card-decode-scheme	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.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.

Job costs and account balances (Zero Stop)

ext-device.konica-minolta.elastic-balance	Allow users an overdraft for a single login 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	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

Network resilience, security, logs

system.network-address	Specify the network IP address or DNS name of the PaperCut MF Application Server that the device uses to make inbound connections.
	This is a global config key.
	• Values: Network IP address or DNS name of the PaperCut MF Application Server used by the device for inbound connections
	Note: For more information, see 4.1.1 Inbound connections to PaperCut MF Application Server.
ext-device.konica-minolta.login.host-based.enabled	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.

For more information, see 4.5 Host-based authentication.

ext-device.konica-minolta.login.host-based-authentication.enabled	Enables secured login for external host-based authentication (if host-based logins are enabled).
	Default: N
	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.
	For more information, see 4.5 Host-based authentication.
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.allow-third-party-pullprint-apps	Allow third party pull print applications to co-exist with PaperCut MF on the device.
	Values: Y, N
	Default: Y
	Setting this to Y will cause PaperCut MF to ignore all third party pull print applications during device registration, allowing them to co-exist with PaperCut MF on the device
	Setting this to N will cause PaperCut MF registration on the device to be halted, if other third party pull print applications are already installed on the device. You will see an error message alerting you to either manually remove all third party pull print applications or allow

	PaperCut MF to do so automatically. PaperCut MF registration on the device will proceed only after all third party pull print applications have been removed.
ext-device.konica-minolta.allow-third-party-scan-apps	Allow third party scan applications to co-exist with PaperCut MF on the device.
	Values: Y, N
	Default: Y
	Setting this to Y will cause PaperCut MF to ignore all third party scan applications during device registration, allowing them to co-exist with PaperCut MF on the device
	Setting this to N will cause PaperCut MF registration on the device to be halted, if other third party scan applications are already installed on the device. You will see an error message alerting you to either manually remove all third party scan applications or allow PaperCut MF to do so automatically. PaperCut MF registration on the device will proceed only after all third party scan applications have been removed.
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.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. Setting this value to "Y" is not recommended for most environments
	Values: Y, N. Default N.
ext-device.konica-minolta.compatibility-mode	Modifies job logging and accounting behavior to accommodate scanning and other embedded applications that rely on the authenticated user name on 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.browser.enabled	Toggle whether the device uses PaperCut MF for i-Option OpenAPI UI or PaperCut MF for the Standard UI.
	Values: Y (i-Option OpenAPI UI), N (Standard UI)
	Default: Y
	Note: Setting this to N is recommended if your device is running the Netfront Browser and you want to upgrade to PaperCut MF 18.2.0 or above. For more information, see 5.14 PaperCut MF 18.2.0 or above does not support Konica Minolta i-Option OpenAPI devices running the NetFront browser.
ext-device.konica-minolta.browser.show-status-bar	Allows the web browser to be used completely in full screen mode, by disabling the status-bar. Set to "Y" to show the status bar, "N" to hide it and display the UI in full screen.
	Values: Y, N. Default: 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.force-app-registration	Determines whether to force applications to re-register on the MFP each time the server is started or any configuration change is made.
	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. Leaving this value as "Y" will cause issues.

	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.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 a 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 a 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)
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.
	Important: If you are using Integrated Scanning, do not set the value to ON_WITHOUT_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.browser.show-sha1-message	Toggle the display of the SHA1 warning message on the PaperCut MF Admin web interface for the device (**Devices > External Device List > Device Details**).
	Values: Y, N
	Default: DEFAULT (Y)
	Note: Setting this to N only hides the SHA1 warning message on the PaperCut MF Admin web interface for the device (**Devices > External Device List > Device Details**). The message continues to be displayed on the device. For more information, see 4.2.1 HTTPS Security (recommended).
ext-device.konica-minolta.use-high-security-port	Specify the port of entry for the SHA 2 HTTPS/ SSL certificate.
	This is a device-specific config key.
	- Values: Y (high security port), N (standard port) - Default: - Y (when installing PaperCut MF 18.3.0 or above for the first time) - N (when upgrading from PaperCut MF 18.2.6 or below)
	Note: This is applicable only to PaperCut MF 18.3.0 or above. For more information, see 4.2.1.3 SHA 1 warning message on PaperCut MF 18.3 or above.
ext-device.konica-minolta.internal-error-handling.enabled	Configure the device to prevent users from accessing the device when PaperCut MF receives the "500: Internal Server Error" from the device.

This is a device-specific config key.

- Values: Y (prevent user access), N (allow user access)
- Default: N

Note:

- This is applicable only when PaperCut MF receives the "500: Internal Server Error" from the device.
  For more information, contact your Reseller or Authorized Solution Center.
- Setting this to Y –
  - locks the device, preventing users from being able to access the device until the "500: Internal Server Error" from the device is resolved.
  - causes the device to display a default message to users, instead of the PaperCut MF Login screen.
    This message can be customized using the config key **ext-device.konica-minolta.internal-error-handling.message**.

ext-device.konica-minolta.internal-error-handling.message	Configure the message displayed on the device when the config key **ext-device.konica-minolta.internal-error-handling.enabled** is enabled (set to **Y**). This is a device-specific config key. • Values: Any text (To add a line break, use *n.*) • Default: "The device is currently experiencing an internal error. Please contact your system administrator." **Note:** This is applicable only when the config key **ext-device.konica-minolta.internal-error-handling.enabled** is enabled (set to **Y**).
Timeouts	
ext-device.konica-minolta.escrow-timeout.mins	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	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.browser.connection-timeout.secs	Specifies any connection timeouts that apply for browser operations in seconds. Default: 30 seconds (1-300 seconds)
ext-device.konica-minolta.timeout.scan-prompt-send.secs	**PaperCut MF Scan Complete timeout:** Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Complete (with the two buttons - **New Scan Document**, **Send**) screen is automatically taken to the PaperCut MF Scan Complete (with scan completed status), and then to the PaperCut MF Home screen. The process of sending the completed scan job to the user (scan transfer) is also automatically initiated. The user continues to be logged in. This is a device-specific config key. • Values: Any positive integer, DEFAULT • Default: DEFAULT (30 seconds)

5 Known Limitations

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

5.1 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.

5.2 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 4.10.

5.3 PageScope Box Operator PC software

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

5.4 Copy Job Logging during User Inactivity

After a copy job is started, from the time stamp of the last notification received, PaperCut MF starts the User Inactivity timeout of one hour (configurable).

- If within this User Inactivity timeout, PaperCut MF DOES receive a logout notification, then from time stamp of the logout notification, PaperCut MF starts the One-hour Job Logging timeout (not configurable). Copy jobs that are completed within this One-hour Job Logging timeout, are accurately logged against the user. Copy jobs that are not completed within this One-hour Job Logging timeout, are unable to be logged against the user.
  For example:

Activity	Time stamps
Last notification	*5 January, 10:00 am*
One-hour User Inactivity timeout	*5 January, 10:00 am – 11:00 am*
Logout notification	*5 January, 10:15 am*
One-hour Job Logging timeout	*5 January, 10:15 – 11:15 am*
Copy job completion	*5 January, 11:00 am → logged* *5 January, 11:16 am → not logged*

- If within this User Inactivity timeout, PaperCut MF DOES NOT receive a logout notification, then from the expiry of this User Inactivity timeout, PaperCut MF starts the 24-hour Job Logging timeout (configurable). Copy jobs that are completed within this 24-hour Job Logging timeout, are accurately logged against the user. Copy jobs that are not completed within this 24-hour Job Logging timeout, are unable to be logged against the user. For example:

Activity	Time stamps
Last notification	*5 January, 10:00 am*
One-hour User Inactivity timeout	*5 January, 10:00 am – 11:00 am*
Logout notification	*N/A*
24-hour Job Logging timeout	*5 January, 11:00 am – 6 January, 11:00 am*
Copy job completion	*6 January, 10:00 am → logged* *6 January, 11:05 am → not logged*

5.5 The "Print All" button on the PaperCut MF screens on the device

The **Print All** button on the following PaperCut MF screens on the device, is available based on the following conditions:

- The PaperCut MF Home screen: The **Print All** button is displayed on this screen, if the device is configured as a release station or is enabled with print release (**Device Details** > **Print Release** > **Enable print release**). For more information, see 4.7 Device .
- The PaperCut MF Print Release screen:
  - If using PaperCut MF 18.1.4 or below, the **Print All** button is displayed on this screen, if the device's settings in the PaperCut MF Admin web interface has **Show button to release all pending jobs** selected (**Device Details** > **Print Release** > **Enable print release** > **Show button to release all pending jobs**). For more information, see 4.7 Device .
  - If using PaperCut MF 18.2.0 or above, the **Select all** checkbox is displayed on this screen, instead of the **Print All** button. For more information, see 4.7 Device .

5.6 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

Please refer to "login.max-stored-sessions" and "login.max-session-age-days" in the Config Editor: 4.10

5.7 Browser Resetting to the Connection Screen

After a period of inactivity on the MFD, the browser will restart and go to the PaperCut connection screen followed by the start screen, which varies depending on the device configuration in PaperCut.

The automatic reset behaviour is controlled by the device and is configurable using:

Administrator setting > Environment setting > Reset setting > Auto reset > Web browser.

Note that hitting "Reset" button on the panel will reset the browser to the initial screen so any screen currently shown will be navigated from and dismissed, this is not configurable.

5.8 Browser screen appears with scroll bars

The embedded software automatically detects maximum display panel resolution advertised by the device and runs at that resolution.

On some devices, a higher resolution value may be returned preventing the screen from being sized correctly and resulting in scroll bars appearing.

This makes the interface harder to use due to excessive scrolling, which can be rectified by manually overriding the configuration settings (ext-device.konica-minolta.browser.screen-height and ext-device.konica-minolta.browser.screen-width) until optimal resolution is achieved. See section 4.10.

5.9 Browser SSL Certificate Installation

The i-Option embedded application supports automatic installation of SSL certificates. This capability is only supported on OpenAPI 4.x devices, and works as follows:

- The certificate assigned to the PaperCut application server (that is the certificate used for the identity of the application server when SSL is enabled) is located and retrieved.
- The certificate will be automatically imported as trusted to the browser of the MFD.
- If the device doesn't support SSL certificate import and an SSL connection to the PaperCut application server is used together with the default self-signed certificate, then the browser

may display warnings about the SSL connections (trust, hostname verification). In such cases, the certificate might need to be manually installed by the administrator.

- If a certificate issued by the standard issuing certificate authorities is used on the PaperCut application server, then the manual steps may not be needed (as the device browser comes with a set of 'standard' trusted certificates).

  Example SSL warning dialog displayed by the NetFront browser:
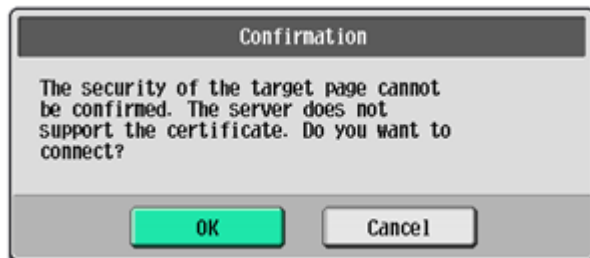
5.10 Browser and connection errors

The browser that's installed on the MFD may show error pop-ups whenever any connectivity errors are detected between the browser and the application server. These are controlled by the browser and the device including any messages that are displayed.

When a pop-up dialog is displayed the device may switch away from the browser to the native user interface. After acknowledging the error dialog the switch back to the browser application is done. It is possible for switch back to not work correctly and either the browser interface not to be brought to the foreground automatically or a blank screen to be shown which can be rectified by hitting "Reset" key to reset the browser to the initial screen.

5.11 Integrated Scans on some devices are always in landscape mode

The orientation of all Integrated Scan jobs (PDF, JPEG, TIFF) produced by some older compact devices (i.e. older devices that do not accept paper sizes higher than Letter or A4) is always in landscape mode, irrespective of the **Orientation** scan settings selected by the user.

To change this behavior for PDF Integrated Scan jobs, ensure the config key **ext-device.konica-minolta.device-type-a4** is set to Y. For more information, see 4.10 Config Editor.

5.12 Duplex, landscape scans using the ADF is unavailable

Using the ADF to scan in duplex, landscape mode, produces incorrectly oriented scan outputs. As a result, duplex, landscape scans can only be done by manually scanning each page via the glass.
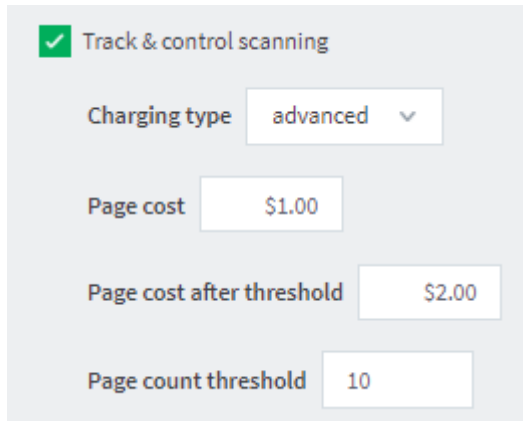
5.13 Impact of Advanced Charging on Integrated Scanning

If you use PaperCut MF's Integrated Scanning and your device is enabled with **Advanced Charging**, then it is recommended you set the following config keys to **N**:

- **ext-device.konica-minolta.browser.scanning-merge-pdf**

- **ext-device.konica-minolta.browser.scanning-merge-tiff**

For more information, see 4.10 Config Editor.

Setting these keys to **Y** prevents the device from being able to implement your Advanced Charging rules while tracking and charging for pages that are subsequently added and scanned by clicking the **New Scan Document** button on the PaperCut MF Scan Complete (with the two buttons – **New Scan Document**, **Send**) screen. Every time a user clicks the **New Scan Document** button and adds more pages to be scanned, they get merged with a previously completed scan job into one PDF or TIFF, as one scan job. For example, if this is your device's **Advanced Charging** setting and you have set the config key **ext-device.konica-minolta.browser.scanning-merge-pdf** / **ext-device.konica-minolta.browser.scanning-merge-tiff** to **Y**, then if a user scans 10 pages and then clicks the **New Scan Document** button and adds another 2 pages, all 12 pages are merged into one PDF/ TIFF and sent to the user:

The user is incorrectly undercharged $12.00 ($1.00 for 12 pages), instead of $14.00 ($1.00 for first 10 pages and $2.00 for all subsequently added pages; 2 in this case).

The PaperCut MF Admin web interface's Job Log page lists multiple scan job rows, one for each time the user clicked the **New Scan Document** button.

5.14 PaperCut MF 18.2.0 or above does not support Konica Minolta i-Option OpenAPI devices running the NetFront browser

PaperCut MF 18.2.0 or above does not support Konica Minolta i-Option OpenAPI devices running the NetFront Browser. Depending on how you wish to resolve this, use any of the following methods:

- If you want to continue to use PaperCut MF on such devices, then ensure to only use 18.1.4 or below. Do not upgrade to PaperCut MF 18.2.0 or above on such devices.
- If you want to upgrade to PaperCut MF 18.2.0 or above, then set the config key **key ext-device.konica-minolta.browser.enabled** to **N** and ensure to switch to the PaperCut embedded solution for the Standard UI on such devices. For more information about PaperCut MF for the Standard UI, contact your reseller or Authorized Solution Center.

5.15 Phonebook contacts

The list of phonebook contacts visible on the MFD can be limited using the config key **system.scan.fax.contact.max-limit**. The default limit is set to 50.

5.16 Performing A5 portrait scan jobs on A4 devices result in unexpected page outputs

On Konica Minolta's A4 devices, PaperCut MF does not support scanning A5 portrait jobs when the A5 pages are placed long-edge-first on the document feeder or flatbed scanner.

A workaround from PaperCut MF 23.0.3 and above is to:

1. Ensure the config key **ext-device.konica-minolta.device-type-a4** is set to Y. For more information, see 4.10 Config Editor.
2. Place the A5 pages short-edge-first (landscape) on the document feeder or flatbed scanner.
3. On the Integrated Scanning settings screen, select "Portrait" as the orientation and "A5" as the paper size.
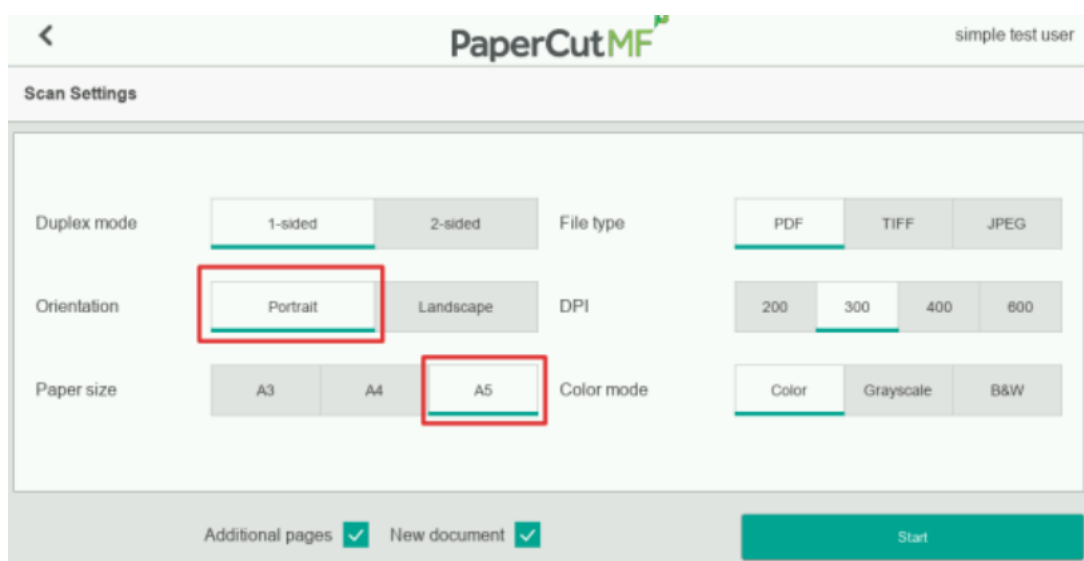
4. Click "Start".

MF will automatically rotate the output to portrait.

6 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) 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. Can the device connect to the PaperCut server on port 9195? 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 9195 (`telnet 1.2.3.4 9195`).

6. Does the device have the latest firmware installed? Connection problems may occur with older firmware versions on some devices.

7. 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 is 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).

When starting the device with no network connection the boot screen may be continuously displayed

Device may not discover an active network connection after a certain point and remain on Konica Minolta boot screen, possible remedy may be to hold the power button on the panel to trigger the "Sub Power Off" mode followed by turning it on and hitting 'Access' button.

Another alternative would be powering off and on using the main power switch.

The device screen is showing an error message "Your 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.

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.

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.

Warning appears on device summary page that states "The i-Option browser interface is not available."

The warning appears if the target device is detected as supporting web browser functionality but it's not been enabled in the configuration. The default (standard UI) interface is being used instead. Advanced device configuration key ext-device.konica-minolta.browser.enabled can be set to Y to enable i-Option (browser) interface. See Configuration Editor 4.10.

Standard Konica Minolta UI is shown instead of PaperCut's web browser UI even though i-Option is setup.

Ensure the device has started successfully by checking device status window on the Device Details > Summary page.

Check that the browser interface is not disabled in PaperCut configuration under Device Details > Advanced Config tab under key ext-device.konica-minolta.browser.enabled (Y for browser/i-Option interface). See Configuration Editor 4.10.

If the configuration looks in order, this may mean that the setup process has determined that the browser functionality is not available on the device, please check you have browser license installed on the MFP and that you have obtained LK101 upgrade kit from Konica Minolta (if applicable), Refer to setup procedure step 13.

Device displays continuously displays "Connecting" message but doesn't connect to PaperCut application server.

The connecting screen is automatically rendered as the first screen on the device which immediately should proceed to the logon screen. The transition is done using JavaScript so if it's disabled in the browser settings this will not occur. Please check the browser settings on the MFP and any relevant networking settings that may impede connectivity to PaperCut application server from the MFP.

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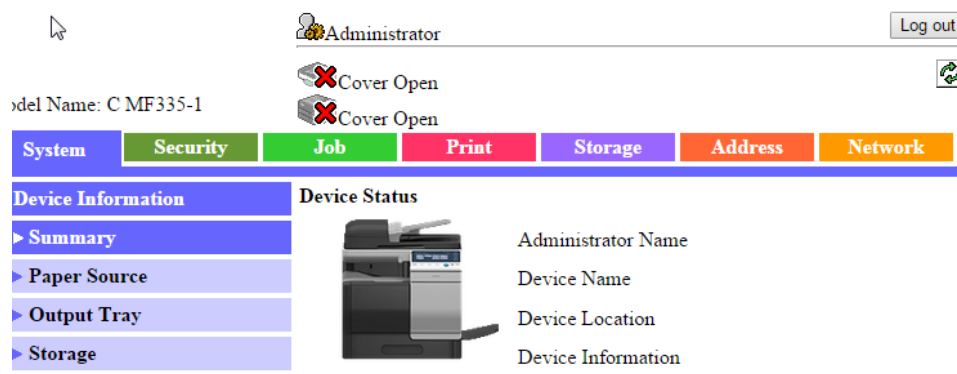
Ensure that the device error is rectified, and then try embedding the device with PaperCut again.

Browser gestures resize the authentication screen.

The web browser on the MFD used for hosting all of the UI supports gestures. The gestures such as "pinch in" or "pinch out" allow the window to be resized and content zoomed.

PaperCut integration instructs the MFP browser not to activate gestures in its own UI as this provides better user experience.

Long document and account names do not use ellipsis.

When running on device models that include NetFront browser any long document names or long account names may not include the terminating ellipsis suffix '…' the values instead are simply truncated.

I am getting the following error message on device screen "Unable to unlock device for use, please try again."

This message may intermittently be shown at the end of the login process into the MFD when done immediately after another user has logged out that had a job finishing at the time.

The error may occur intermittently anywhere between 10 seconds to a minute after the job has finished and another login has started.

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.

When the UI is shown, a message is displayed: "Certificate credentials could not be verified"

This message is usually indicative of the MFD browser not having the certificate used by PaperCut application server in its trusted certificate store.

When managing the device using OpenAPI4 device type the certificate is usually automatically imported.

Depending on the type of browser installed on the device and the model/firmware it may be possible to manually import the certificate.

In the case of models using NetFront browser, the certificate can be manually imported by logging to the device as administrator and starting the browser manually then importing the certificate via the browser UI (URLInput button).

Normally in this case the certificate needs to be extracted out of PaperCut and hosted on any web server that can be accessed from the MFD. A URL to the hosted certificate is used to import the certificate into the browser.

I've plugged the card reader in but it doesn't seem to activate the copier?

The MFDs often have multiple USB ports. Some are suitable for use with a card reader, some are not. Please ensure that you have tried all the USB ports on the machine.

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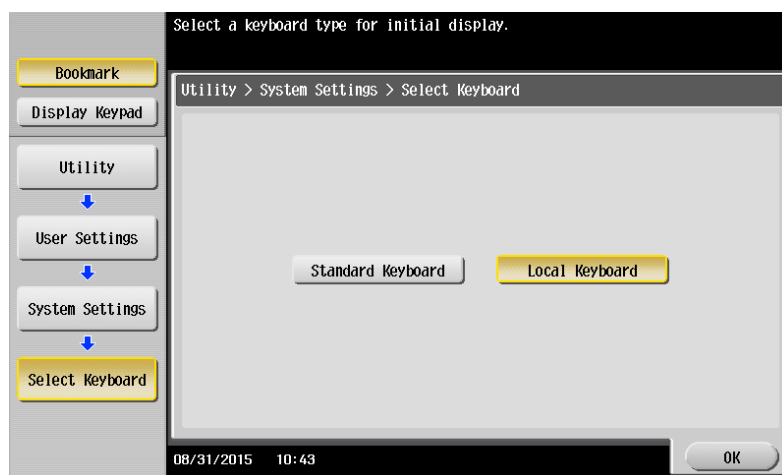
Why is a user's name displayed with a number in parenthesis appended to it?

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'.

7 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 this device" 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.

8 Appendix A: Device screens
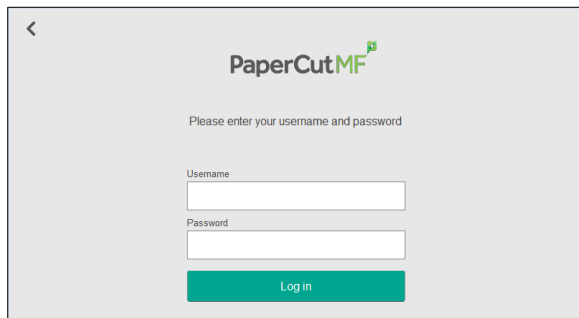
Figure 1 User authentication:
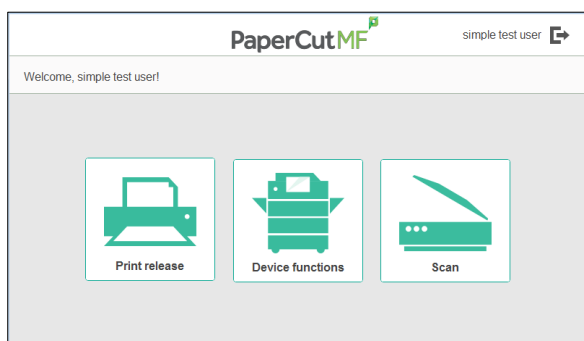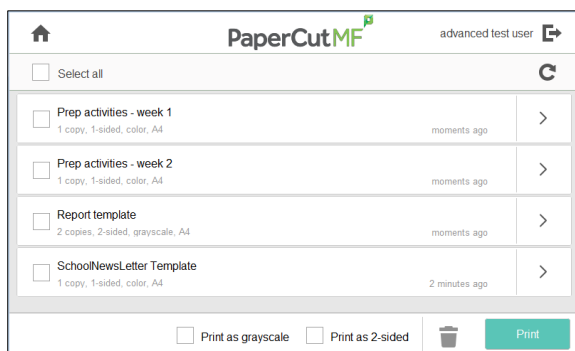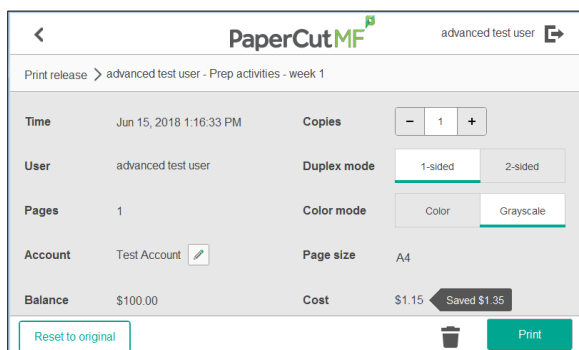
Figure 2 Home:

Figure 3 Secure Print Release:

Figure 4 Charging of jobs:
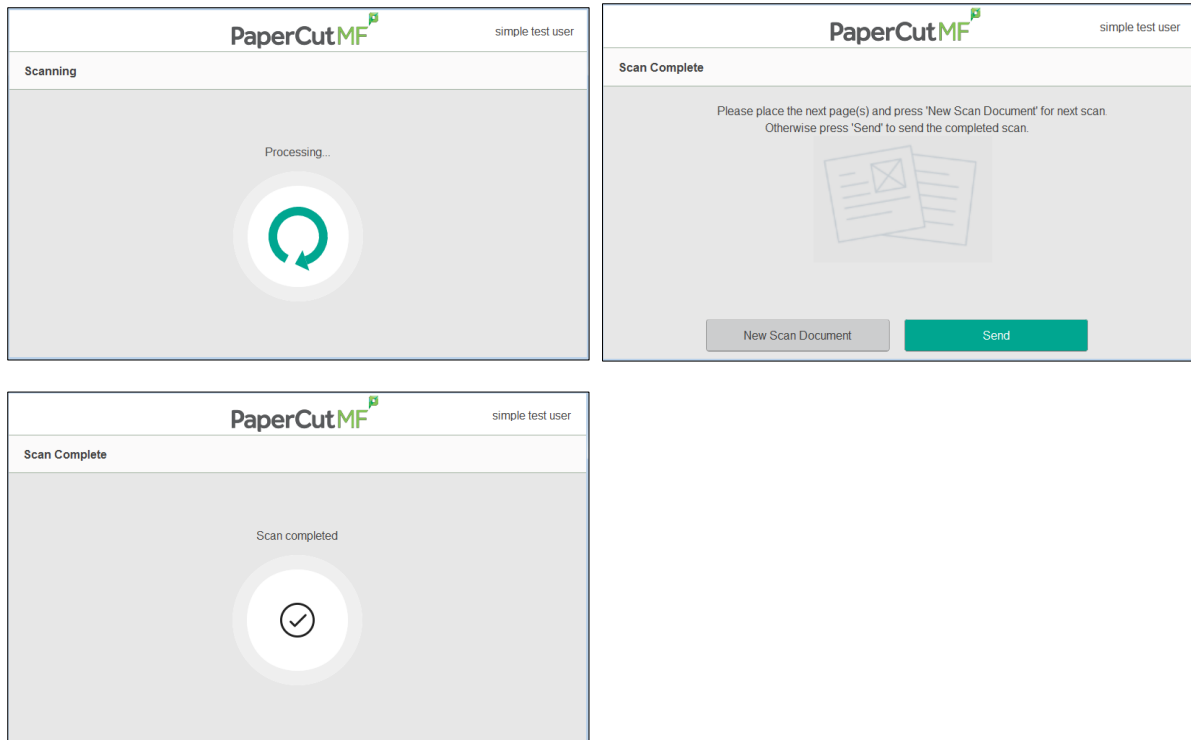
Figure 5 PaperCut MF Integrated Scanning:

Basic experience:

Figure 6 Empty state - Add a recipient using manual entry

Figure 7 Manual entry - Enter a Fax number, Recipient name and Recipient company name.

Figure 8 Multiple recipients

Advanced experience

Figure 9 Empty state - Add a recipient using manual entry or select a recipient from the phonebook

Figure 10 Manual entry - First manual entry can be edited.

Figure 11 Select a recipient using search on the phone book and add to the scrollable list.