PaperCut MF - Ricoh SmartSDK Embedded Manual

Contents

ƒv

1 Document revision history

Published date or release	Details of changes made
22.0.0	Added 4.8.4.5 File Uploading; Added config keys ext-device.ricoh.scan.upload.async-disabled and ext-device.ricoh.scan.upload.concurrent-limit to 4.12 Config Editor
20.0.0	Deleted (2.4.1.4 Configure the device’s usage control settings; some steps in 2.4.2.4 Configure the first part of the device’s usage control settings); Added section under 2.4.2.8 for enhanced deployment.
19.2.0	Document restructure (to support ***PaperCut MF Ricoh SmartSDK Printer Only***)
19.1.0	Document restructure
19.0.0	3 Overview; 4.3.3.1 Launch the Remote Operation Client; 8.4 Held print jobs at the device; 8.6 SNMP; 9.1 Config Editor; 9.6 ICE Print Cloud print jobs
18.3.7	4.4 Bypassing PaperCut MF; 5 Uninstall PaperCut MF
23 November 2018	8.3 Swipe card authentication; 9.2 Connecting supported card readers
18.2.0	2 Which version do I install?; 3 Overview; 4 Installation; 5 Upgrading to a newer version; 6 Post-install testing; 7 Configuration; 8 Advanced configuration

2 Installation

This section covers the installation of *PaperCut MF – Ricoh (SmartSDK).*

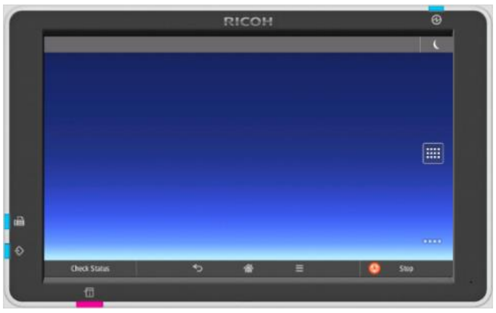
2.1 Supported devices

Ensure that the devices on the network are listed as supported devices on the [PaperCut MF for Ricoh]() page.

2.2 Compatible devices

Ensure that the supported Ricoh devices on the network are compatible with PaperCut's embedded software solutions: *PaperCut MF – Ricoh (SmartSDK):*

- they are running Embedded Software Architecture (ESA) SmartSDK version 2.12 or above, and,
- they have a second-generation Smart Operation Panel running Android, without any hard keys:



Note: This manual is only relevant to supported and compatible Ricoh devices. For more information on PaperCut's embedded software solutions for other devices and platforms, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut MF Admin web interface, on the **About** page.

2.3 System requirements

Ensure that the following system requirements are met:

- The following entities are available:
    - Physical device – administrator and user access, and credentials
    - Device's web interface – administrator access, URL, and credentials
    - PaperCut MF Ricoh Remote Operation Client (i.e. ROC) – administrator access
    - PaperCut MF Admin web interface – administrator access, URL, and credentials
- The latest version of the PaperCut MF Application Server is installed and running on the network. For more information, see the [PaperCut MF manual]().
  Note: The minimum compatible version of the PaperCut MF Application Server for multi-function devices is 19.1.0 or above.
  Note: The minimum compatible version of the PaperCut MF Application Server for single function devices is 19.2.0 or above.
- The networking/firewall configuration allows:
    - Inbound connections to the PaperCut MF Application Server from the devices on the configured ports. For example:
        - 9191 (TCP/HTTP)
        - 9192 (SSL/TLS/HTTPS)

  - Inbound and outbound connections to and from the PaperCut MF Ricoh Remote Operation Client (ROC) on the following ports:
    - 51443
    - 80
    - 443

2.4 Setup procedure

Depending on your environment and your device, you can install PaperCut MF (i.e. device registration and integration) using any of the following options:

- 2.4.1 Install PaperCut MF with the Ricoh Remote Operation Client (ROC)
- 2.4.2 Install PaperCut MF without the Ricoh Remote Operation Client (ROC)

2.4.1 Install PaperCut MF with the Ricoh Remote Operation Client (ROC)

Note: This is only applicable to:

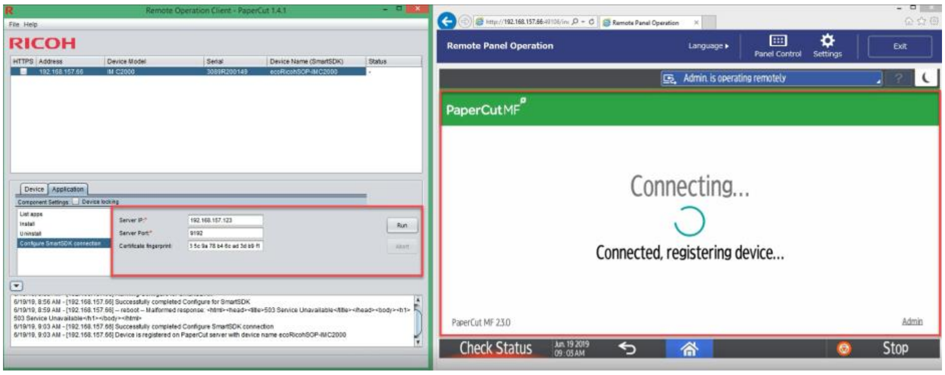
- post-Spring 2017 devices, or
- pre-Spring 2017 devices, with a Java card installed.

PaperCut MF ships with the PaperCut MF Ricoh Remote Operation Client (i.e. ROC), which enables you to install PaperCut MF:

- remotely, instead of physically on each device, AND
- in bulk, instead of one device at a time.

Thereby, increasing your operational efficiency, while also minimizing human errors.

Watch this video to see how to install PaperCut MF using the ROC:



HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	IM C2000	3089R200149	ecoRicohSOP-IMC2000	-

Server IP:* 192.168.157.123
Server Port:* 9192
Certificate fingerprint: 1 5c 9a 78 b4 6c ad 3d b9 f1

```
6/19/19, 8:56 AM - [192.168.157.66] Successfully completed Configure for SmartSDK
6/19/19, 8:59 AM - [192.168.157.66] -- reboot -- Malformed response: <html><head><title>503 Service Unavailable</title></head><body><h1>
503 Service Unavailable</h1></body></html>
6/19/19, 9:03 AM - [192.168.157.66] Successfully completed Configure SmartSDK connection
6/19/19, 9:03 AM - [192.168.157.66] Device is registered on PaperCut server with device name ecoRicohSOP-IMC2000
```

Connecting...

Connected, registering device...

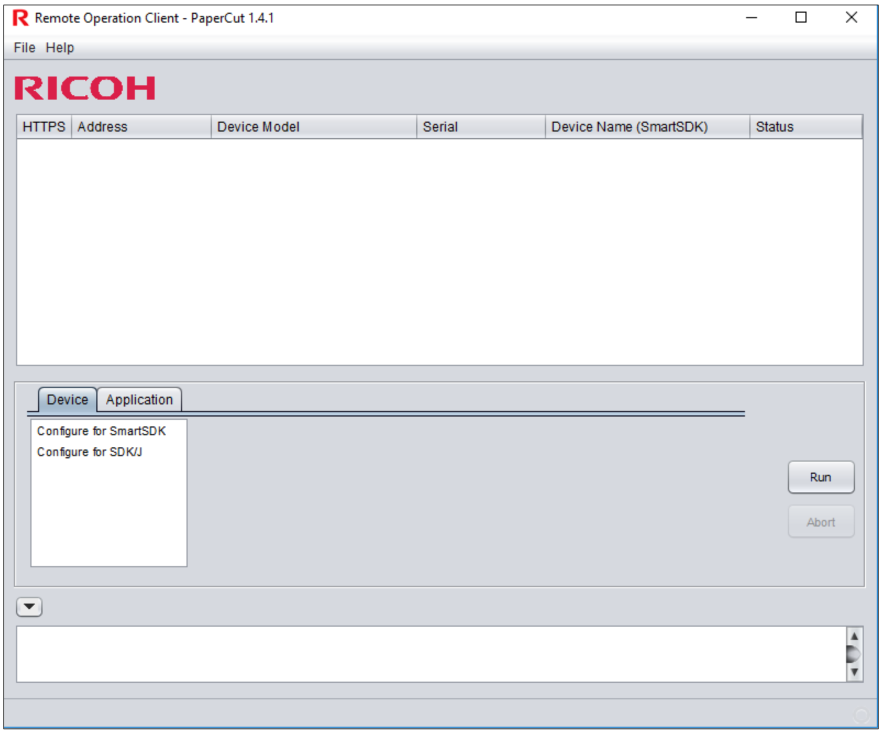
To install PaperCut MF (i.e. device registration and integration) with the ROC:

- 2.4.1.1 Start the Ricoh Remote Operation Client (ROC)
- 2.4.1.2 Create the device list
- 2.4.1.3 Configure the device's user access permission settings
- 2.4.1.4 Install the PaperCut MF embedded application
- 2.4.1.5 Enable communication with the PaperCut MF Application Server

2.4.1.1 Start the Ricoh Remote Operation Client (ROC)

To start the ROC:

1. Log in to the machine running your PaperCut MF Application Server.
2. Navigate to:
   `[PaperCut MF Install Location]\providers\hardware\ricoh\remote-operation-client\`
3. Depending on your environment (OS), launch the PaperCut MF Ricoh Remote Operation Client:
   - In a Windows environment, run the `remote-operation-client.bat` file with administrator privileges.
   - In a UNIX environment (macOS, Linux), launch the terminal and run the `sudo ./remote-operation-client` command.



2.4.1.2 Create the device list

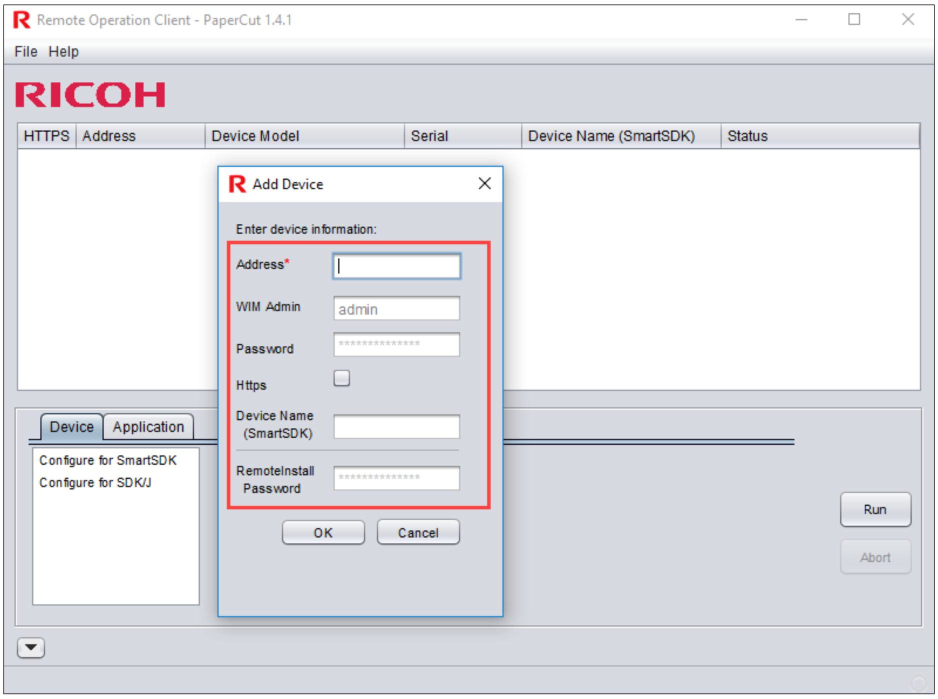
To create a list of devices on the ROC:

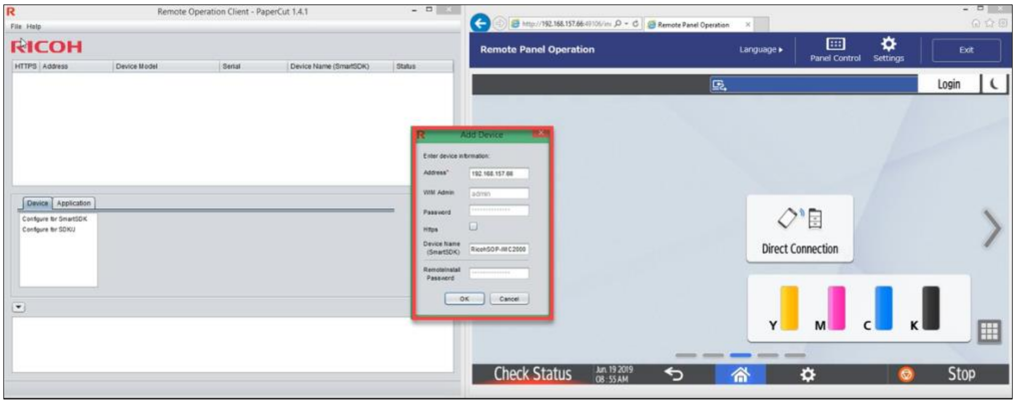
1. To add multiple devices at once:
   a. Ensure the **devices.csv**:
      - contains valid details about the devices under the following CSV headers, in this order:
        IP, **Password**, **userwim**, **pwdwim**, **https**, **Device Name (SmartSDK)**.
        For more information, see 8 Appendix A: Creating a list of devices on the Ricoh Remote Operation Client (ROC).
      - is available in the following location:
        `[PaperCut MF Install Location]\providers\hardware\ricoh\remote-operation-client\device-list`

      Note: PaperCut MF includes a template **devices.csv** that is pre-formatted with the required CSV headers, in the required location.
   b. On the ROC, navigate to **File > Import lst File**.
   c. Locate and select the **devices.csv** file.

    d. Click **Import.**
    e. It is recommended that you apply the required security to this **devices.csv** file (either purge it or save it in another secure location), because it contains administrative credentials of your devices.

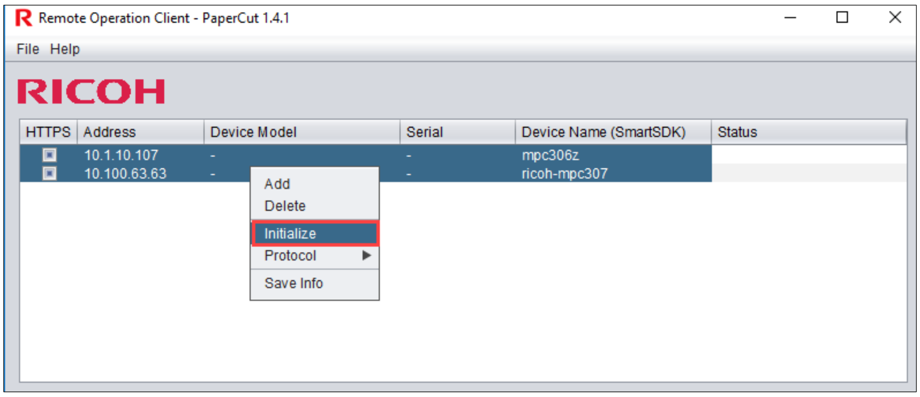
2. To add one device at a time:
    a. On the ROC, navigate to **File > Add**.
    b. Enter the required details for each device:
    Address, WIM Admin, Password, Https, Device Name (SmartSDK), RemoteInstall Password.
    For more information, see 8 Appendix A: Creating a list of devices on the Ricoh Remote Operation Client (ROC).



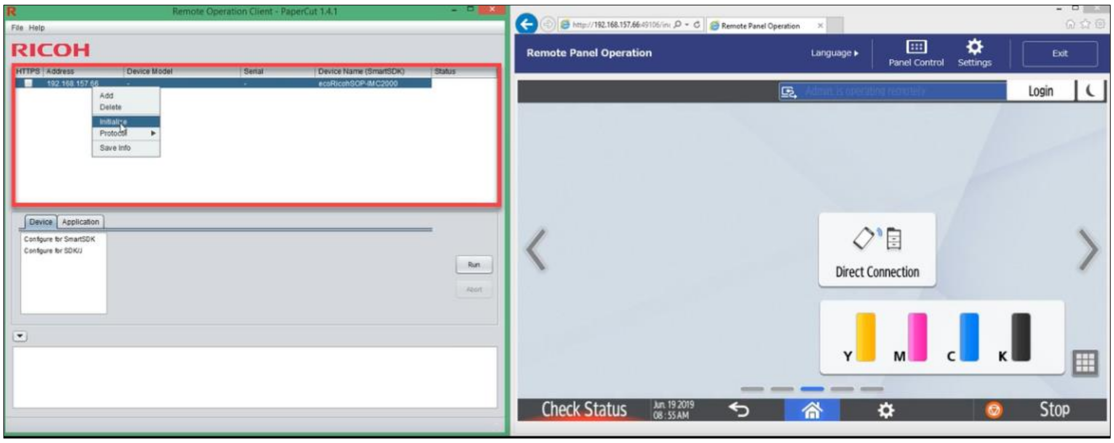


    c. Click **OK**.
    d. Repeat this for each device.

3. Verify that the ROC'S table displays rows of added devices, with some columns populated.
4. Select the required devices, and right-click them.
5. Click **Initialize**.

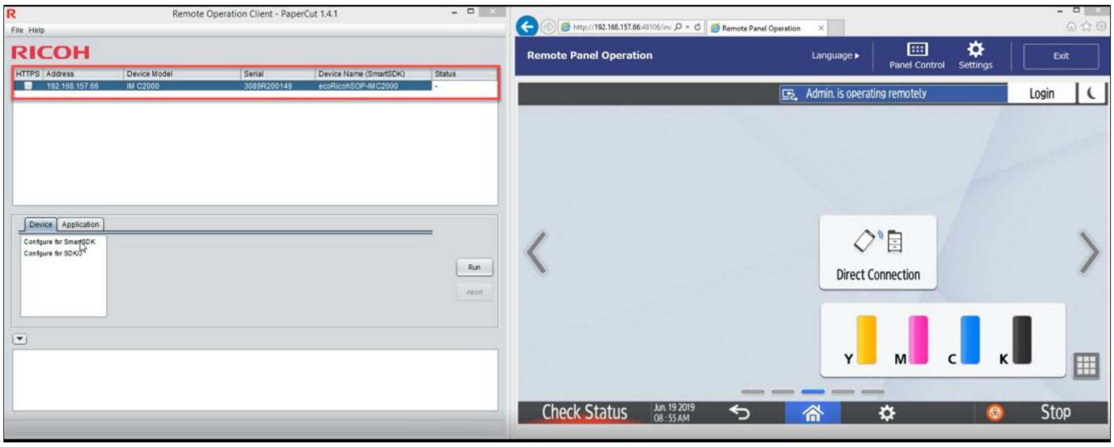


HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	10.1.10.107	-	-	mpc306z	
☐	10.100.63.63	-	-	ricoh-mpc307	



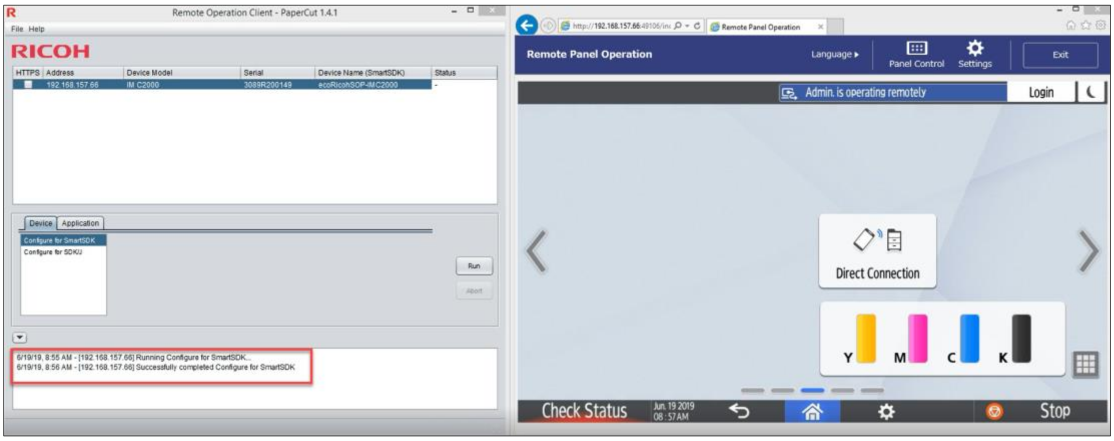
HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	-	-	ecoRicohSOP-IMC2000	

6. Verify that:
   - ROC table's **Device Model, Serial** columns – are populated accurately for every device.
   - ROC table's **Status** column – is not populated with any errors for any device.
     Note: If the ROC table's **Status** column displays errors for any device, then see 6.2 Ricoh Remote Operation Client (ROC) Status errors.



HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	IM C2000	3089R200149	ecoRicohSOP-IMC2000	-

7. With the required devices still selected, navigate to **Device > Configure for SmartSDK.**
8. Click **Run**.
9. Verify that the ROC'S Console displays the status **Successfully completed Configure for SmartSDK** for every selected device.
   Note: If the ROC'S Console displays errors, then see 6.3 Ricoh Remote Operation Client (ROC) Console errors.



HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	IM C2000	3089R200149	ecoRicohSOP-IMC2000	-

```
6/19/19, 8:55 AM - [192.168.157.66] Running Configure for SmartSDK...
6/19/19, 8:56 AM - [192.168.157.66] Successfully completed Configure for SmartSDK
```

2.4.1.3 Configure the device's user access permission settings

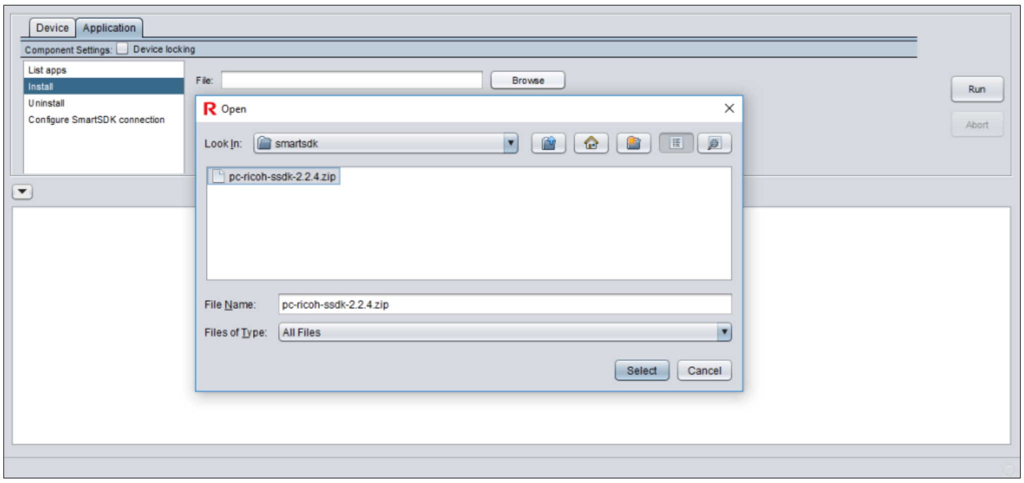
To ensure that authenticated, non-administrative users can access required device jobs, you must configure the device's user access permission settings. You can do this using any one of the following options:

- To remotely configure the device's user access permission settings:
    1. Log in to the device's web interface as an administrator.
    2. Navigate to **Device Management > Configuration > User Authentication Management**.
    3. In **User Authentication Management**, select **Custom Authentication**.
    4. In **Available Functions**, deselect each of the following:
        - **Copier**
          Note: This is only applicable to multi-function devices.
        - **Printer**
        - **Other Function(s)**
- To physically configure the device's user access permission settings:
    1. Access the physical device.
    2. Log in as an administrator.
    3. Navigate to **User Tools > System Settings > Administrator Tools > User Authentication Management** > **Custom Authentication**
    4. In **Available Functions**, deselect each of the following:
        - **Copier**
          Note: This is only applicable to multi-function devices.
        - **Printer**
        - **Other Function(s)**

2.4.1.4 Install the PaperCut MF embedded application

To install the PaperCut MF embedded application on the list of devices that have been created on the ROC:

1. On the ROC, with the required devices still selected, navigate to **Application > Install.**
2. Click **Browse**.
3. Navigate to the following location:
   `[PaperCut MF Install Location]\providers\hardware\ricoh\smartsdk`
4. Select the PaperCut MF embedded application ZIP file. For example, *pc-ricoh-ssdk-2.3.0.zip.*



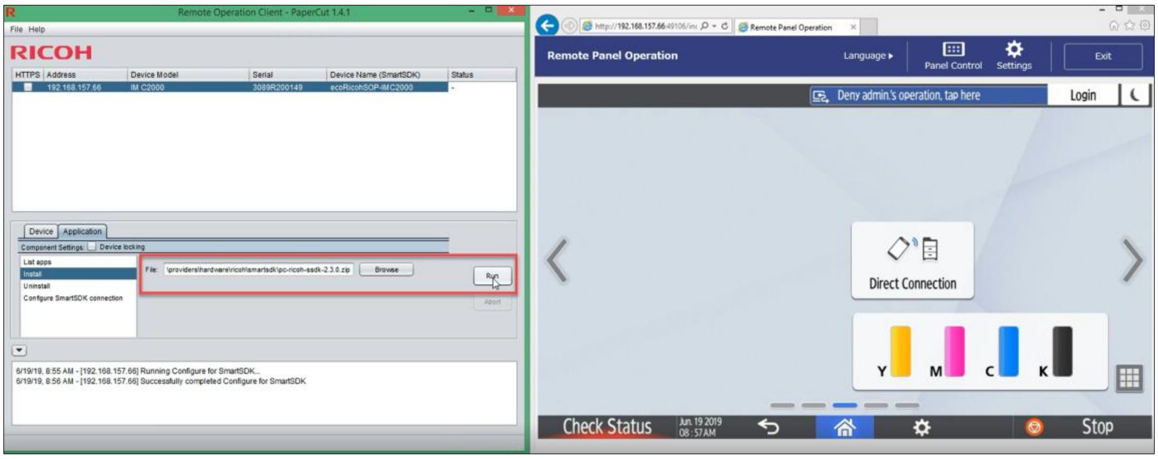
Look In: smartsdk

pc-ricoh-ssdk-2.2.4.zip

File Name: pc-ricoh-ssdk-2.2.4.zip

Files of Type: All Files

5. Click **Run**.



File: \providers\hardware\ricoh\smartsdk\pc-ricoh-ssdk-2.3.0.zip

```
6/19/19, 8:55 AM - [192.168.157.66] Running Configure for SmartSDK...
6/19/19, 8:56 AM - [192.168.157.66] Successfully completed Configure for SmartSDK
```

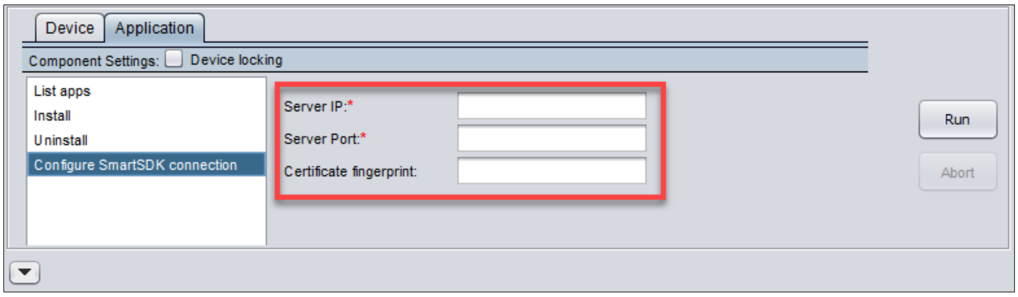
6. Verify that the ROC'S Console displays the status **Successfully installed PaperCut MF v<x.x.x>** for every selected device.

2.4.1.5 Enable communication with the PaperCut MF Application Server

To enable communication between the PaperCut MF Application Server and the devices that have been installed with the PaperCut MF embedded application:

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. Click **Log out**.
6. On the ROC, check the checkboxes of the devices that have been installed with the PaperCut MF embedded application.
7. Navigate to **Application > Configure SmartSDK connection**.
8. Enter the required details of the PaperCut MF Application Server:
    - **Server IP** — The IP or network address of the PaperCut MF Application Server. If using a hostname, make sure it is fully-qualified so it can be correctly resolved.
    - **Server Port** — The port used to communicate with the PaperCut MF Application Server. It is recommended that you use an HTTPS/ SSL port, which is 9192 by default.

- **Certificate fingerprint** — If the **Server Port** is an SSL port, then enter the space separated, SHA1 fingerprint of the PaperCut MF Application Server's certificate. For example, *09 2F E2 37 70 1E 59 B7 3D E8 41 40 66 DA 51 6E 58 CB 9A 44*.



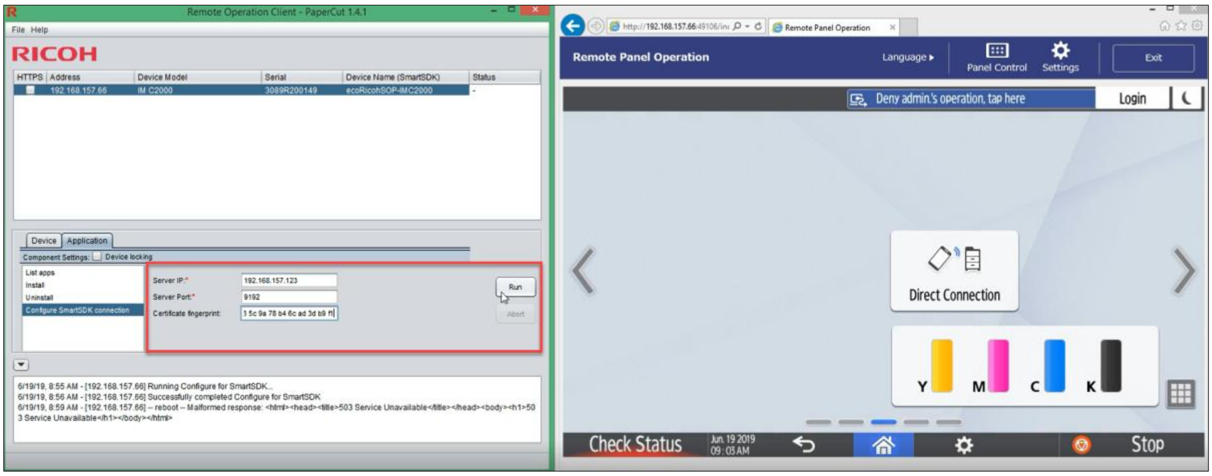
9. Click **Run**.

   Note: If the **Server Port** is an HTTPS/ SSL port and **Certificate fingerprint** is either missing or is invalid, then the device displays an error.

   You can resolve it either:

   - for all devices at once (by entering the **Certificate fingerprint** on the ROC), or
   - for each device (by accepting the certificate on each individual device).

   For more information, see the PaperCut MF manual, Where is the "Fingerprint" of my Server?



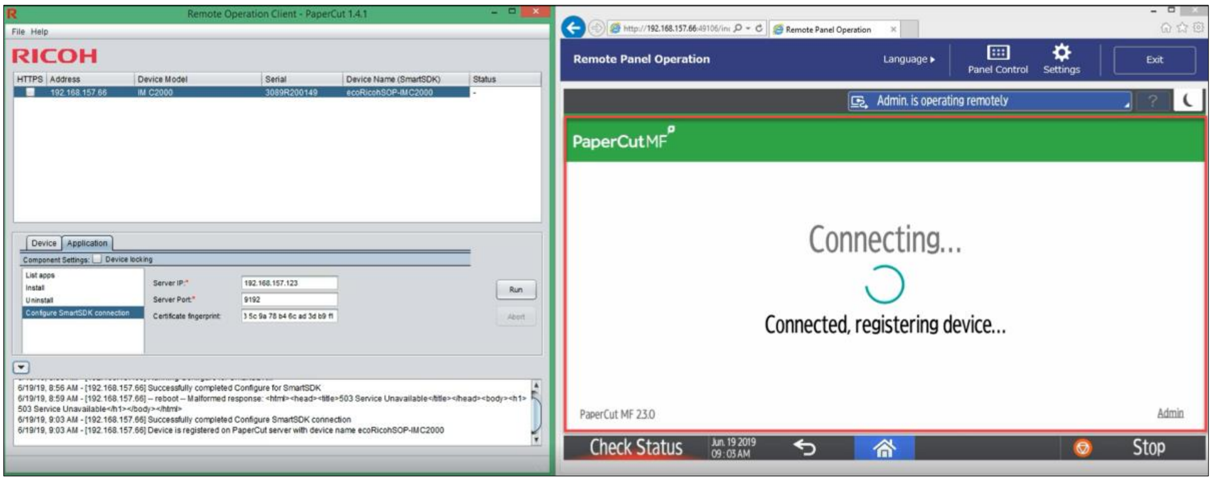
HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	IM C2000	3089R200149	ecoRicohSOP-IMC2000	-

Server IP:* 192.168.157.123

Server Port:* 9192

Certificate fingerprint: 3 5c 9a 78 b4 6c ad 3d b9 f1

```
6/19/19, 8:55 AM - [192.168.157.66] Running Configure for SmartSDK...
6/19/19, 8:56 AM - [192.168.157.66] Successfully completed Configure for SmartSDK
6/19/19, 8:59 AM - [192.168.157.66] -- reboot -- Malformed response: <html><head><title>503 Service Unavailable</title></head><body><h1>50
3 Service Unavailable</h1></body></html>
```



Connecting...

Connected, registering device...

HTTPS	Address	Device Model	Serial	Device Name (SmartSDK)	Status
☐	192.168.157.66	IM C2000	3089R200149	ecoRicohSOP-IMC2000	-

Server IP:* 192.168.157.123

Server Port:* 9192

Certificate fingerprint: 3 5c 9a 78 b4 6c ad 3d b9 f1

```
6/19/19, 8:56 AM - [192.168.157.66] Successfully completed Configure for SmartSDK
6/19/19, 8:59 AM - [192.168.157.66] -- reboot -- Malformed response: <html><head><title>503 Service Unavailable</title></head><body><h1>
503 Service Unavailable</h1></body></html>
6/19/19, 9:03 AM - [192.168.157.66] Successfully completed Configure SmartSDK connection
6/19/19, 9:03 AM - [192.168.157.66] Device is registered on PaperCut server with device name ecoRicohSOP-IMC2000
```

2.4.2 Install PaperCut MF without the Ricoh Remote Operation Client (ROC)

Note: This is the only available option for pre-Spring 2017 multi-function devices without a Java card installed.

If you are unable to use the PaperCut MF Ricoh Remote Operation Client (i.e. ROC) to install PaperCut MF, you can do so without the ROC. To install PaperCut MF (i.e. device registration and integration) without the ROC:

- 2.4.2.1 Configure the device's authentication settings
- 2.4.2.2 Configure the device's administrator access permission settings
- 2.4.2.3 Configure the device's user access permission settings
- 2.4.2.4 Configure the first part of the device's usage control settings
- 2.4.2.5 Configure the device's user archive settings
- 2.4.2.6 Configure the device's scanner archive settings
- 2.4.2.7 Configure the application authentication management settings
- 2.4.2.8 Install the PaperCut MF embed application
- 2.4.2.9 Enable communication with the PaperCut MF Application Server
    - 2.4.2.9.1 Remotely configure multiple devices
    - 2.4.2.9.2 Manually configure each device
- 2.4.2.10 Configure the second part of the device's usage control settings

2.4.2.1 Configure the device's authentication settings

Note: This requires a Ricoh service technician.

You must configure the device's authentication settings to ensure that PaperCut MF is the only authentication application on the device. This is because having multiple authentication applications results in conflict and causes the device to behave erratically.

To remotely configure the device's authentication settings:

1. Access the physical device as a Ricoh service technician.
2. Set the **System Parameters** as follows:
    a. Set the **Optional Counter Type > External Optional Counter Type** to **0**.
    b. Set the **Access Control > SDK Certification Device > bit 0** to **1**.
    c. Set the **MF KeyCard > Job Permit Setting** to **1**.

2.4.2.2 Configure the device's administrator access permission settings

To ensure that only authenticated administrators can access certain device jobs, you must configure the device's administrator access permission settings. You can do this using any one of the following options:

- To remotely configure the device's administrator access permission settings:
    1. Log in to the device's web interface as an administrator.
    2. Navigate to **Device Management** > **Configuration** > **Administrator Authentication Management.**

   3. Set each of the following to **On**; and select the available settings for each:
      - **User Management**
      - **Machine Management**
      - **Network Management**
      - **File Management**
- To physically configure the device's administrator access permission settings:
   1. Access the physical device.
   2. Log in as an administrator.
   3. Navigate to **User Tools > System Settings > Administrator Tools > Administrator Authentication Management.**
   4. Set each of the following to **On**; and select the available settings for each:
      - **User Management**
      - **Machine Management**
      - **Network Management**
      - **File Management**

2.4.2.3 Configure the device's user access permission settings

To ensure that authenticated, non-administrative users can access required device jobs, you must configure the device's user access permission settings. You can do this using any one of the following options:

- To remotely configure the device's user access permission settings:
   1. Log in to the device's web interface as an administrator.
   2. Navigate to **Device Management > Configuration > User Authentication Management**.
   3. In **User Authentication Management**, select **Custom Authentication**.
   4. In **Available Functions**, deselect each of the following:
      - **Copier**
        Note: This is only applicable to multi-function devices.
      - **Printer**
      - **Other Function(s)**
- To physically configure the device's user access permission settings:
   1. Access the physical device.
   2. Log in as an administrator.
   3. Navigate to **User Tools > System Settings > Administrator Tools > User Authentication Management** > **Custom Authentication**
   4. In **Available Functions**, deselect each of the following:
      - **Copier**
        Note: This is only applicable to multi-function devices.
      - **Printer**
      - **Other Function(s)**

2.4.2.4 Configure the first part of the device's usage control settings

To ensure that PaperCut MF has control of required device jobs, you must configure the device's usage control settings. You can do this using any one of the following options:

- To remotely configure the device's usage control settings:
   1. Log in to the device's web interface as an administrator.
   2. Navigate to **Device Management > Configuration > Print Volume Use Limitation:**

      a. In **Machine Action When Limit Is Reached**, select **Stop Job.**

- To physically configure the device's usage control settings:
    1. Access the physical device.
    2. Log in as an administrator.
    3. Navigate to **User Tools > System Settings > Administrator Tools.**
    4. In **Machine Action When Limit Is Reached**, select **Stop Job.**

2.4.2.5 Configure the device's user archive settings

You must configure the device's user archive settings to prevent it from failing when its archive is full (i.e. enable it to purge session details of the oldest user). You can do this using any one of the following options:

- To remotely configure the device's user archive settings:
    1. Log in to the device's web interface as an administrator.
    2. Navigate to **Device Management > Address Book > Maintenance.**
    3. In **Auto Delete User in Address Book,** select **On.**
- To physically configure the device's user archive settings:
    1. Access the physical device.
    2. Log in as an administrator.
    3. Navigate to **User Tools > System Settings > Administrator Tools.**
    4. In **Auto Delete User in Address Book,** select **On.**

2.4.2.6 Configure the device's scanner archive settings

Note: This is only applicable to multi-function devices.

You must configure the device's scanner to prevent it from failing when its archive is full. You can do this using any one of the following options:

- To remotely configure the device's scanner archive settings:
    1. Log in to the device's web interface as an administrator.
    2. Navigate to **Device Management > Configuration > Scanner > General Settings.**
    3. In **Print & Delete Scanner Journal,** select **Do not Print: Delete Oldest.**
- To physically configure the device's scanner archive settings:
    1. Access the physical device.
    2. Log in as an administrator.
    3. Navigate to **User Tools > Scanner Features > General Settings.**
    4. In **Print & Delete Scanner Journal,** select **Do not Print: Delete Oldest.**

2.4.2.7 Configure the application authentication management settings

To ensure that jobs are tracked and user permissions are applied, the following values should be set to ON by default.

1. Access the physical device.
2. Log in as an administrator.
3. Navigate to **User Tools > System Settings > Administrator Tools > Application Authentication Management.**
4. Select **On** for all of the following device jobs:
    - *Copier*
    - *Printer*

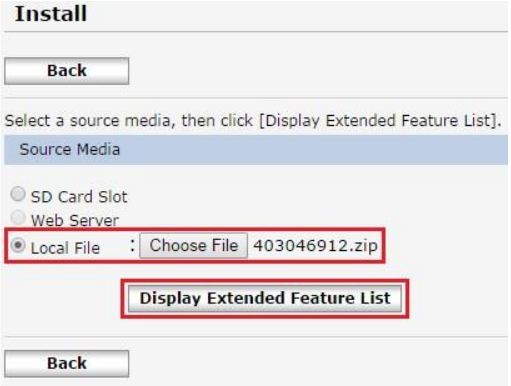
- *Document Server*
- *Fax*
- *Scanner*

Note: Copier device jobs should be set to ON for Color Copy Restrictions to work. Tracking and controlling certain device jobs can be disabled as needed, see 6.7.2 Disabling PaperCut MF from tracking and controlling specific device jobs.

2.4.2.8 Install the PaperCut MF embedded application

To remotely install the PaperCut MF embedded application on a device:

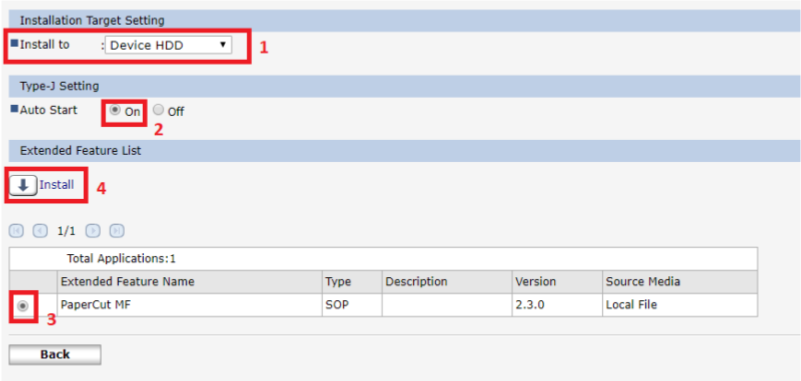
1. Log in to the device's web interface as an administrator.
2. Navigate to **Device Management > Configuration > Extended Feature Settings > Install.**
3. Select **Local File**.
4. Click **Choose File**.
5. Navigate to the following location:
   `[PaperCut MF Install Location]\providers\hardware\ricoh\smartsdk`
7. Select the PaperCut MF embedded application ZIP file. For example, *pc-ricoh-ssdk-2.2.4.zip.*
8. Click **Display Extended Feature List**.



Select a source media, then click [Display Extended Feature List].

● Local File : 403046912.zip

9. In **Installation Target Setting > Install to**, select **Device HDD**.
10. In **Type-J Setting > Auto Start**, select **On**.
11. In **Extended Feature List**:
    a. first select the **PaperCut MF** row
    b. then click **Install**



Install to : Device HDD

Auto Start ● On ○ Off

Total Applications:1

	Extended Feature Name	Type	Description	Version	Source Media
●	PaperCut MF	SOP		2.3.0	Local File

12. In the confirmation dialog, ensure the installation options are accurate; then click **Ok**.

2.4.2.9 Enable communication with the PaperCut MF Application Server

To enable communication between the PaperCut MF Application Server and the devices that have been installed with the PaperCut MF embedded application:

1. Log into 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. Click **Log out**.
6. You can use any of the following options:
    - 2.4.2.9.1 Remotely configure multiple devices
    - 2.4.2.9.2 Manually configure each device

2.4.2.9.1 Remotely configure 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.

Note: Ricoh devices can be added as “Staged” at any time, and are deployed automatically when the physical device, with embedded installed, calls into the PaperCut MF server for the first time. For more information, see the Enhanced Deployment Project web page.

2.4.2.9.2 Manually configure each device

1. Access the physical device.
2. On the Configure screen, enter the required details of the PaperCut MF Application Server:
    - **Device name** — The unique name of the device.
      Note: The device is registered with this name in the PaperCut MF Admin web interface.
    - **Server hostname/IP** — The IP or network address of the PaperCut MF Application Server. If using a hostname, make sure it is fully-qualified so it can be correctly resolved.
    - **Port** — The port used to communicate with the PaperCut MF Application Server. It is recommended that you use an HTTPS/ SSL port, which is 9192 by default.
3. Click **Save changes**.
   Note: If the **Server Port** is an HTTPS/ SSL port, then the device prompts you to accept the PaperCut MF Application Server’s certificate. For more information, see the PaperCut MF manual, Where is the “Fingerprint” of my Server?
4. Repeat this for each device.

2.4.2.10 Configure the second part of the device's usage control settings

To ensure that PaperCut MF has control of required device jobs, you must configure the device's usage control settings:

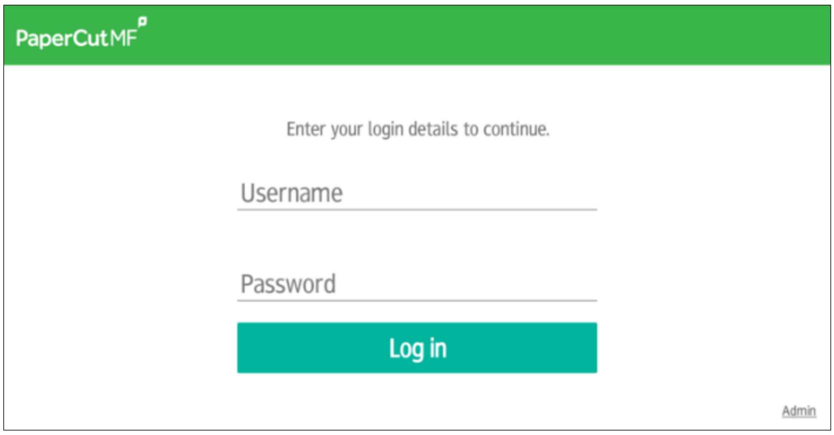
1. Access the physical device.
2. Log in to the device as a user.
3. Navigate to any device job (scan, copy, fax, on-device printing).
4. You can configure the device's usage control settings using any one of the following options:
    - To physically configure the device's usage control settings:
        i. Log in to the device as an administrator.
        ii. Navigate to **User Tools > System Settings > Administrator Tools > Enhanced Print Volume Use Limitation.**
        iii. In **Tracking Permission**, select **On**.
        iv. In **Stop Printing**, select **On.**
    - To remotely configure the device's usage control settings:
        i. Log in to the device's web interface as an administrator.
        ii. Navigate to **Device Management > Configuration > Print Volume Use Limitation.**
        iii. In **Tracking Permission**, select **On**.
        iv. In **Stop Printing**, select **On.**

2.5 Verify PaperCut MF installation

To verify that PaperCut MF is successfully installed (i.e. device registration and integration):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Verify the following:
    - the **TYPE** column displays the following as required:
        - ***Ricoh (SmartSDK) Printer Only*** – for single function devices
        - ***Ricoh (SmartSDK)*** – for multi-function devices
    - the required devices are listed without any errors in the **STATUS** column.

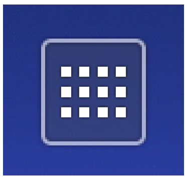
   Note: If these details are not displayed as outlined, see 6.4 Device Status "Connecting to server…".
4. Click **Log out**.
5. Access the physical device.
6. Verify that the first screen on the device displays the PaperCut MF Login screen:



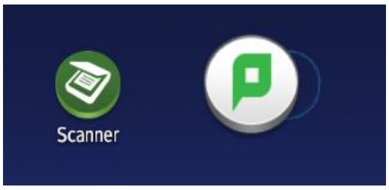
2.6 Configure the device's Home screen

To enable users to easily navigate to and access PaperCut MF screens, ensure the device's Home screen displays the PaperCut MF icon:

1. Log in to the device as an administrator (see 6.6 Accessing administrative jobs).
2. On the device's panel, click **Home.**
3. On the device's Home screen, click **All apps**.



4. On the device's Apps screen, click and hold the **PaperCut MF** icon until the screen switches to the device's Home screen.



5. Drag the **PaperCut MF** icon to the device's Home screen, and then release it.

2.7 Configure the device's timeout

A user who is detected as being idle (on a PaperCut MF screen or a non-PaperCut MF device screen) is automatically logged out after a certain interval of time, based on the device's timeout settings.

To configure the device's timeout settings:

1. Access the physical device.
2. Log in as an administrator.
3. Navigate to **User Tools > System Settings > Timer Settings > Sleep Timer.**
   Note: To access and configure this remotely, log in to the device's web interface as an administrator and then navigate to **Device Management > Configuration > Timer.**
4. Configure the **System Auto Reset Timer**; and disable **Auto Logout Timer.**
5. Navigate to **User Tools > Screen Features > Screen Device Settings**
6. In **Function Priority**, select **PaperCut MF.**
   Note: This is to ensure that after the **System Auto Reset Timer** elapses, the PaperCut MF embedded application does not recede into the background.

2.8 Upgrade the PaperCut MF embedded application on the device

- Multi-function devices running the PaperCut MF embedded application 1.0.8 or below, cannot be seamlessly upgraded to a newer version; and must be first uninstalled before newer version is installed. Other settings previously configured are not retained.
- Multi-function devices running the PaperCut MF embedded application 1.0.9 or above can be seamlessly upgraded to a newer version, while also retaining all other settings previously configured (see 2 Installation). Before upgrading, ensure that the device is connected to the PaperCut MF Application Server. After upgrading, verify that the PaperCut MF embedded application's version number reflects the expected value.

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 for *PaperCut MF – Ricoh (SmartSDK).*

- 3.2 Jobs with a simple workflow
- 3.3 Jobs with an advanced workflow

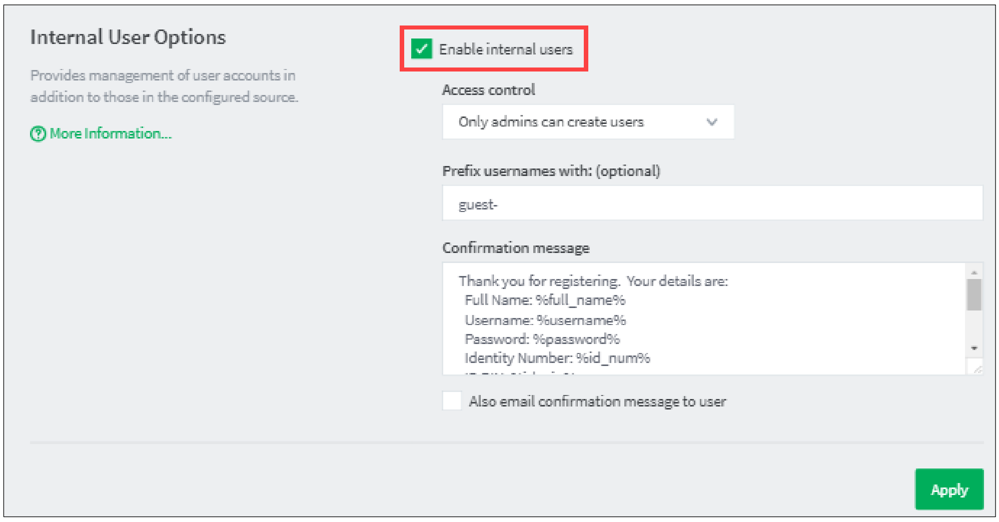
3.1 Test preparation: create test users

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

- **Simple test user** – A user who performs jobs using a simple workflow (i.e. without the task of cost allocation).
- **Advanced test user** – A user who performs jobs using an advanced workflow (i.e. with the task of cost allocation).

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**.



Internal User Options

Provides management of user accounts in addition to those in the configured source.

More Information...

☑ Enable internal users

Access control: Only admins can create users

Prefix usernames with: (optional): guest-

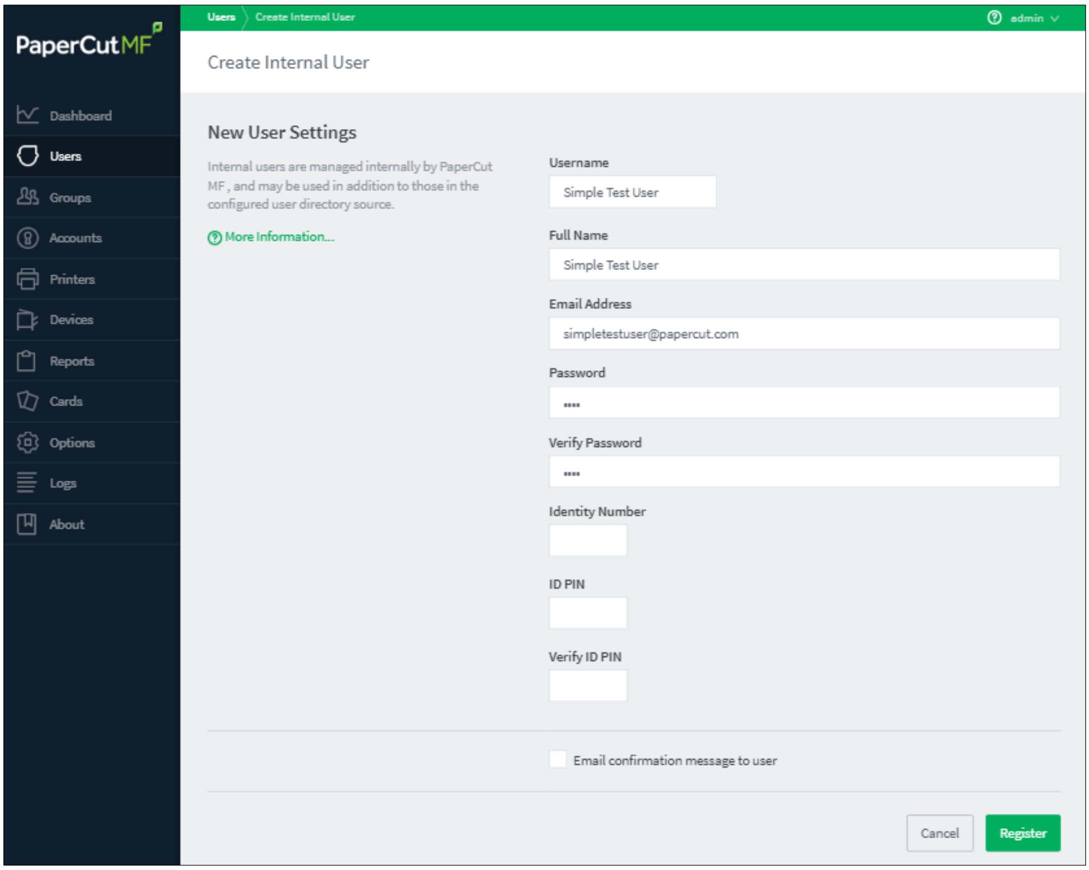
Confirmation message:

Thank you for registering. Your details are:
Full Name: %full_name%
Username: %username%
Password: %password%
Identity Number: %id_num%

☐ Also email confirmation message to user

5. Navigate to **Users**.
6. Click **Create internal user...**

7. Enter the required details for the test users as required (simple test user, advanced test user):



Create Internal User

New User Settings

Internal users are managed internally by PaperCut MF , and may be used in addition to those in the configured user directory source.

Username: Simple Test User
Full Name: Simple Test User
Email Address: simpletestuser@papercut.com
Password: ····
Verify Password: ····
Identity Number:
ID PIN:
Verify ID PIN:

☐ Email confirmation message to user

8. Click **Register**.

3.2 Jobs with a simple workflow

Jobs using a simple workflow are jobs that are performed without the task of cost allocation. It does not involve providing the simple test user with a choice of accounts to choose from.

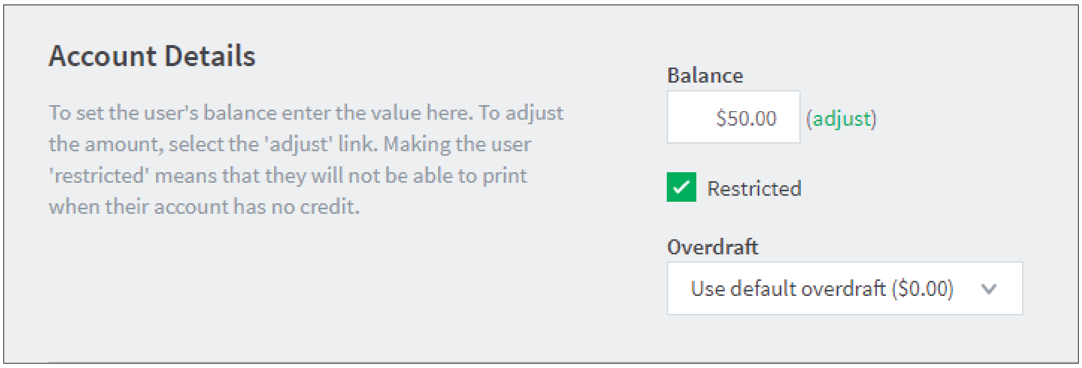
3.2.1 Test preparation: configure simple test user

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:**



Account Details

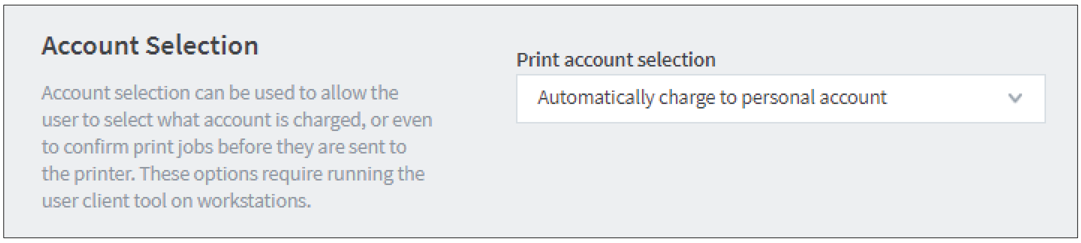
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: $50.00 (adjust)

☑ Restricted

Overdraft: Use default overdraft ($0.00)

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



Account Selection

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

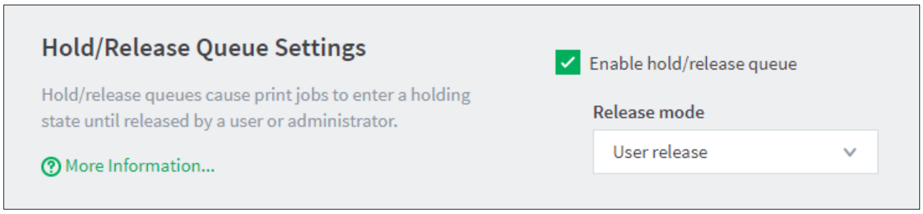
Print account selection: Automatically charge to personal account

6. Click **Apply**.

3.2.2 Simple printing

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**.

    Hold/Release Queue Settings

    Hold/release queues cause print jobs to enter a holding state until released by a user or administrator.

    More Information...

    ☑ Enable hold/release queue

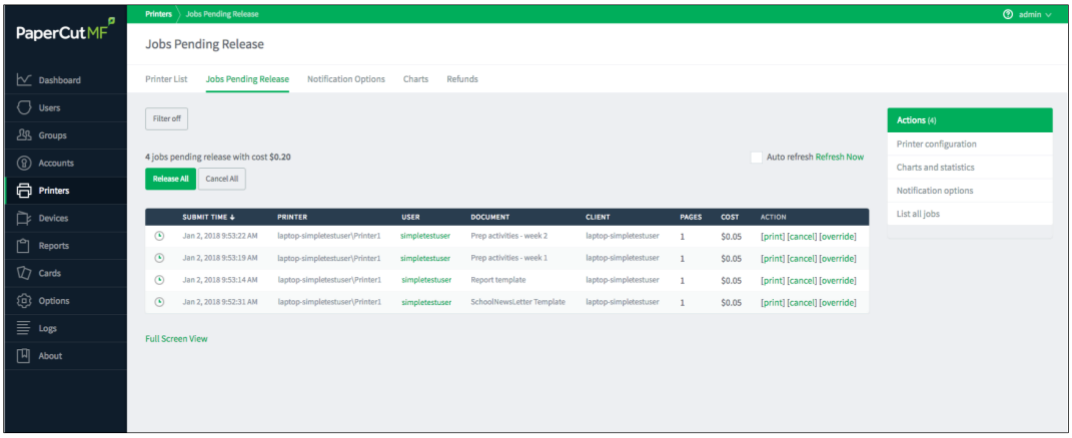
    Release mode: User release

    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 required 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 a simple print job:

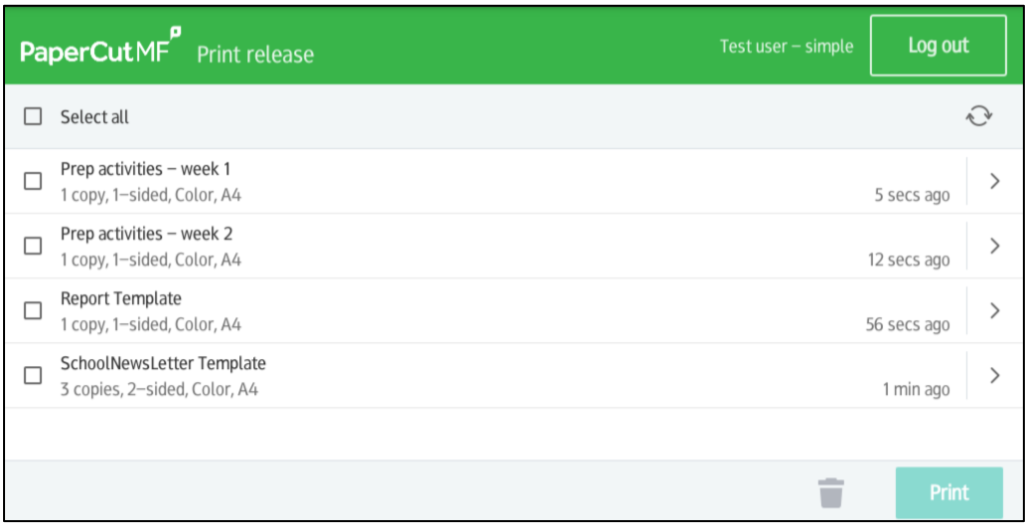
1. Log in to a computer as the simple test user.
2. Print a few jobs to the source queue that was selected in the **Devices > External Device List > Device Details > Print Release > Enable print release** area of the device being tested.
3. Log in to the PaperCut MF Admin web interface.
4. Navigate to **Printers > Jobs Pending Release**.
5. Verify that the print jobs for the simple test user are being held and listed:



4 jobs pending release with cost $0.20

	SUBMIT TIME ↓	PRINTER	USER	DOCUMENT	CLIENT	PAGES	COST	ACTION
	Jan 2, 2018 9:53:22 AM	laptop-simpletestuser\Printer1	simpletestuser	Prep activities - week 2	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
	Jan 2, 2018 9:53:19 AM	laptop-simpletestuser\Printer1	simpletestuser	Prep activities - week 1	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
	Jan 2, 2018 9:53:14 AM	laptop-simpletestuser\Printer1	simpletestuser	Report template	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
	Jan 2, 2018 9:52:31 AM	laptop-simpletestuser\Printer1	simpletestuser	SchoolNewsLetter Template	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]

6. Log out of the PaperCut MF Admin web interface.
7. Log in to the device as the simple test user.
8. Select **Print Release**.
9. Verify that the print jobs for the simple test user are being held and listed:



☐ Select all

☐ Prep activities – week 1
1 copy, 1–sided, Color, A4 — 5 secs ago

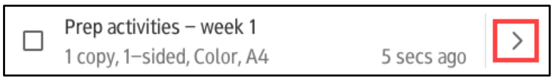
☐ Prep activities – week 2
1 copy, 1–sided, Color, A4 — 12 secs ago

☐ Report Template
1 copy, 1–sided, Color, A4 — 56 secs ago

☐ SchoolNewsLetter Template
3 copies, 2–sided, Color, A4 — 1 min ago

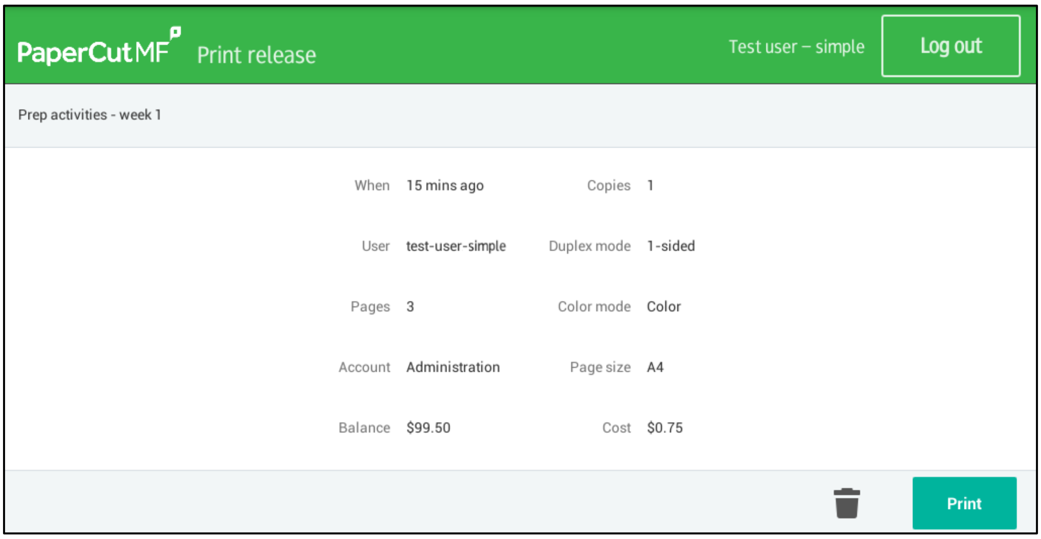
10. To release one or many held print jobs at once, select all the required held print jobs and click **Print**.
11. To delete one or many held print jobs at once, select all the required held print jobs and click the **Bin** icon.

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



☐ Prep activities – week 1
1 copy, 1–sided, Color, A4 5 secs ago

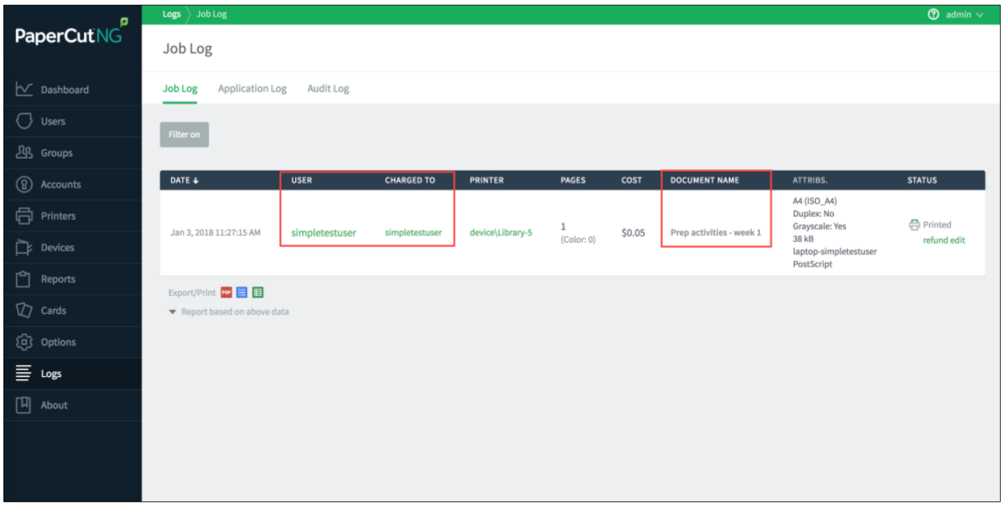
Details of the held print job are displayed:



Prep activities - week 1

When	15 mins ago	Copies	1
User	test-user-simple	Duplex mode	1-sided
Pages	3	Color mode	Color
Account	Administration	Page size	A4
Balance	$99.50	Cost	$0.75

13. Log out of the device.
14. Log in to the PaperCut MF Admin web interface.
15. Navigate to **Logs**.
16. 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:



DATE ↓	USER	CHARGED TO	PRINTER	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Jan 3, 2018 11:27:15 AM	simpletestuser	simpletestuser	device\Library-5	1 (Color: 0)	$0.05	Prep activities - week 1	A4 (ISO_A4) Duplex: No Grayscale: Yes 38 kB laptop-simpletestuser PostScript	Printed refund edit

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

3.2.3 Simple copying or on-device printing

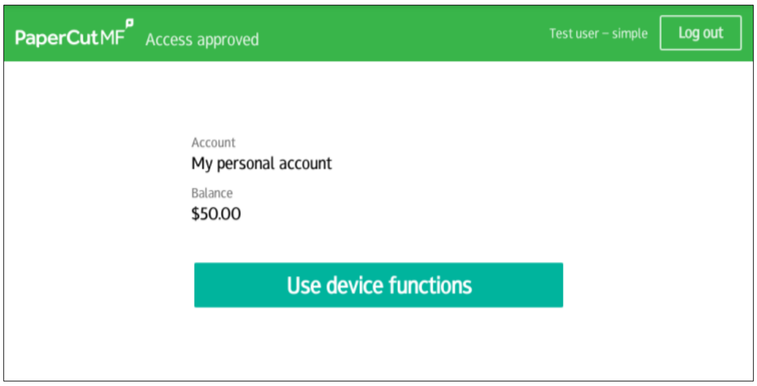
To test simple copying or on-device printing, ensure the following test preparation requirements are met:

- **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
- **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 required 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.

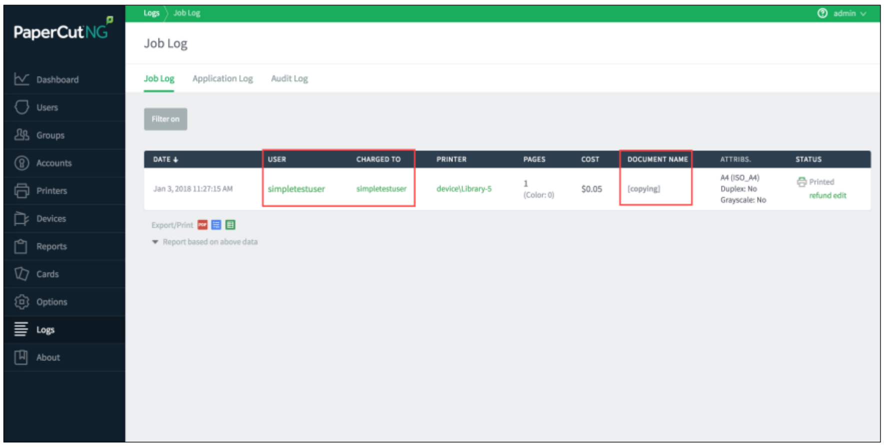
To test a simple copy or on-device print job:

1. Log in to the device as the simple test user.
2. Verify that the simple test user is not provided with a choice of accounts to choose from, and the job is charged to the simple test user's default My Personal Account:



Account
My personal account
Balance
$50.00

3. Complete the simple copy or on-device print job.
4. Log out of the device.
5. Log in to the PaperCut MF Admin web interface.
6. Navigate to **Logs**.
7. After the job 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:



DATE ↓	USER	CHARGED TO	PRINTER	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Jan 3, 2018 11:27:15 AM	simpletestuser	simpletestuser	device\Library-5	1 (Color: 0)	$0.05	[copying]	A4 (ISO_A4) Duplex: No Grayscale: No	Printed refund edit

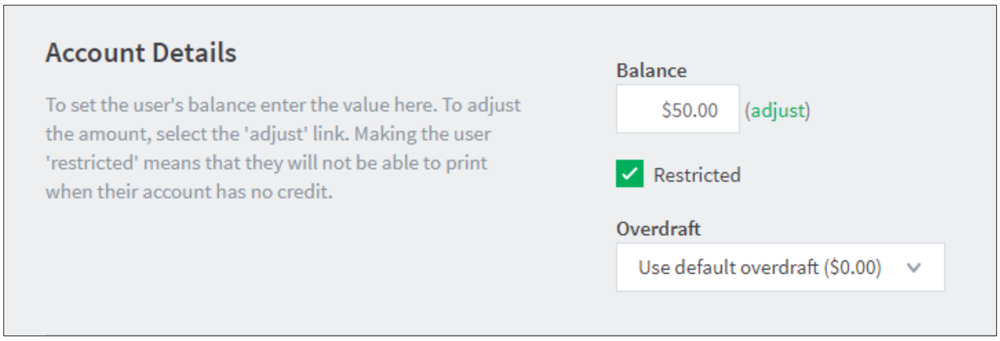
8. Log out of the PaperCut MF Admin web interface.

3.3 Jobs with an advanced workflow

Jobs using an advanced workflow are jobs that are performed with the task of cost allocation. It involves providing the advanced test user with a choice of accounts to choose from. The job is charged to the account that is selected by the advanced test user.

To test a job (such as, a copy job or an on-device print job) using an advanced workflow, 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:**



Account Details

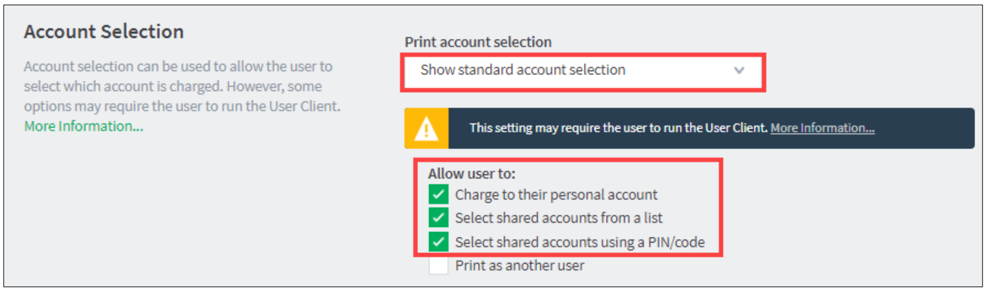
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: $50.00 (adjust)

☑ Restricted

Overdraft: Use default overdraft ($0.00)

  5. In the **Account Selection** area's **Print account selection**, select **Show standard account selection** and select the required options:



Account Selection

Account selection can be used to allow the user to select which account is charged. However, some options may require the user to run the User Client. More Information...

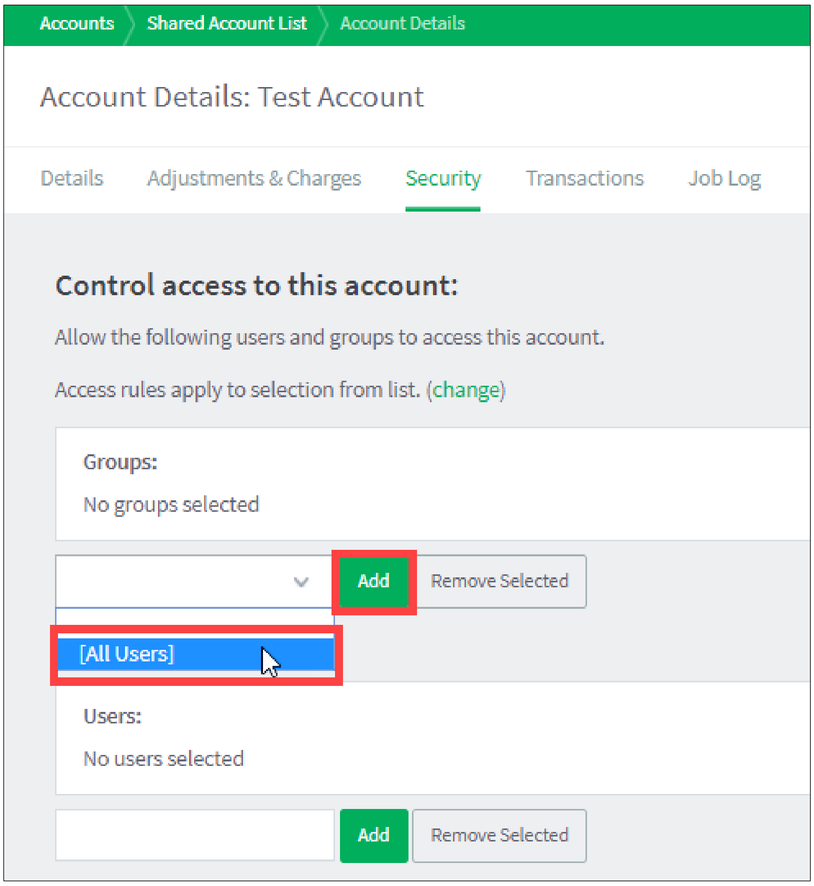
Print account selection: Show standard account selection

This setting may require the user to run the User Client. More Information...

Allow user to:
☑ Charge to their personal account
☑ Select shared accounts from a list
☑ Select shared accounts using a PIN/code
☐ Print as another user

  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 required 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 1).
  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] and click **Add**:



Account Details: Test Account

Control access to this account:

Allow the following users and groups to access this account.

Access rules apply to selection from list. (change)

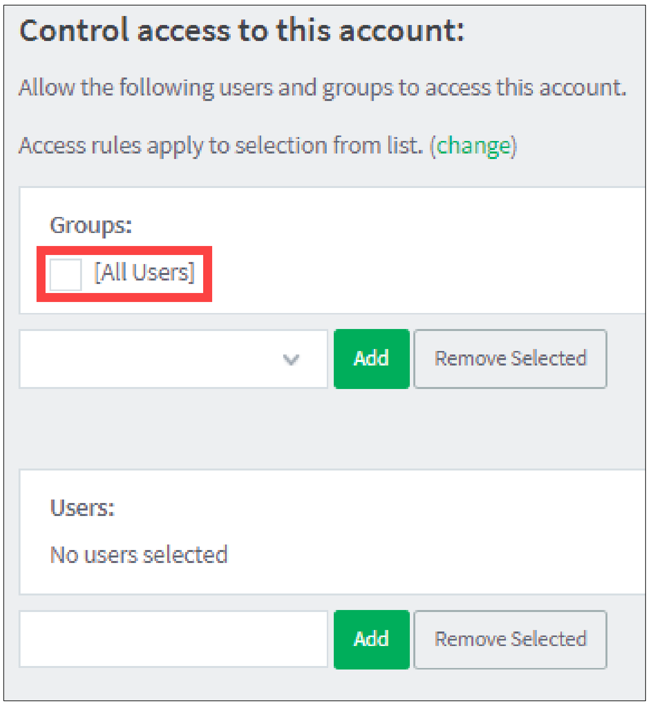
Groups:

No groups selected

Users:

No users selected

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



Control access to this account:

Allow the following users and groups to access this account.

Access rules apply to selection from list. (change)

Groups:

☐ [All Users]

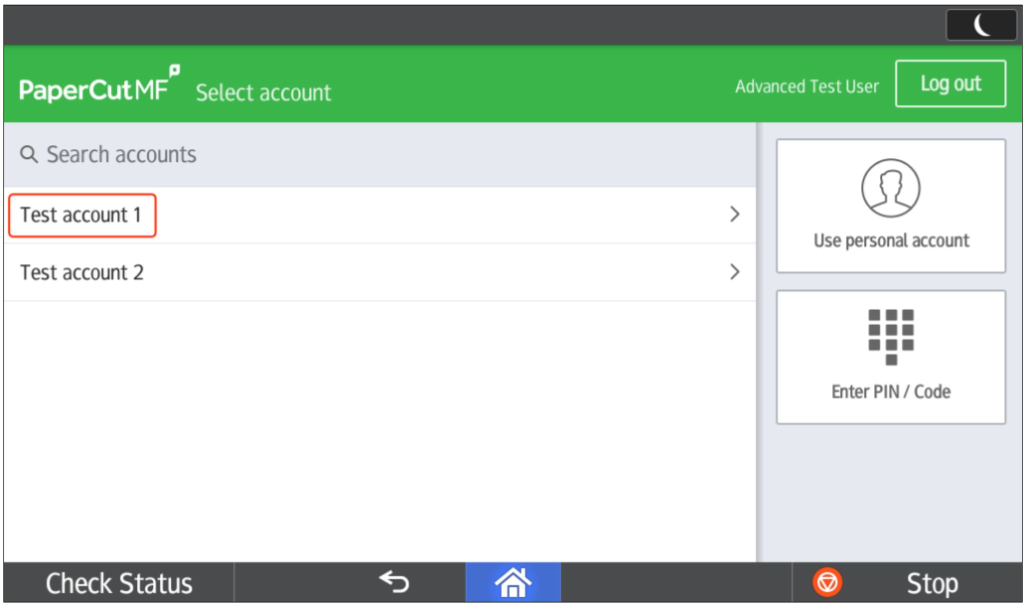
Users:

No users selected

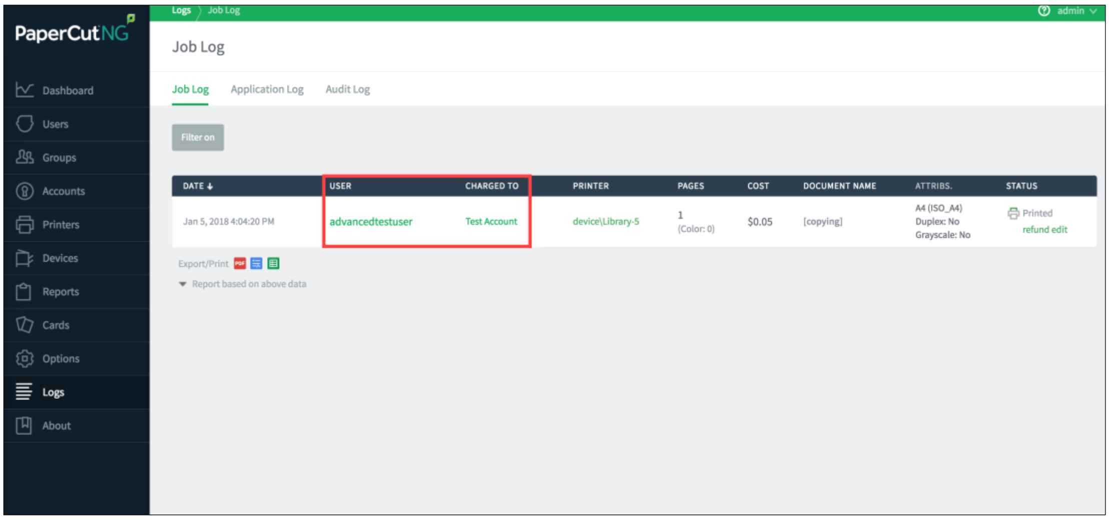
To test a job (such as, a copy job or an on-device print job) using an advanced workflow:

1. Log in to the device as the advanced test user.

2. Verify that the advanced test user is provided with a choice of accounts to choose from:



3. Select the required account, Test account 1.
4. Complete the job by following the device's workflow.
5. The job is charged to the account selected by the advanced test user, Test account 1.
6. Log out of the device.
7. Log in to the PaperCut MF Admin web interface.
8. Navigate to **Logs**.
9. After the job 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:



DATE ↓	USER	CHARGED TO	PRINTER	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Jan 5, 2018 4:04:20 PM	advancedtestuser	Test Account	device\Library-5	1 (Color: 0)	$0.05	[copying]	A4 (ISO_A4) Duplex: No Grayscale: No	Printed refund edit

10. 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.

This section covers the configuration changes that can be made to the default settings of *PaperCut MF – Ricoh (SmartSDK).*

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**.

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:

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 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:

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

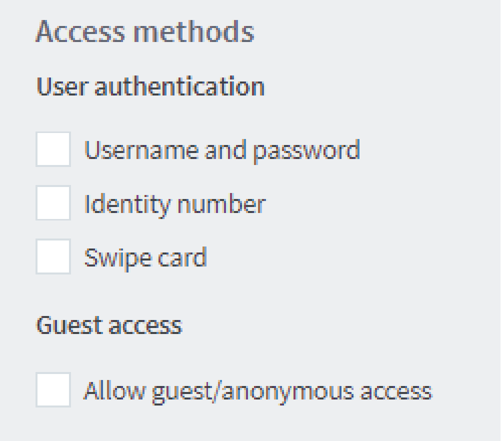
Note: Ensure that:

- PaperCut MF is the only authentication application on the device (see 2.4.2.1 Configure the device's authentication settings)
- the device's user archive settings are configured as required (see 2.4.2.5 Configure the device's user archive settings)

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 required device.
   The available user authentication options are in the **Device Details** page's **External Device Settings** area:

   Access methods

   User authentication

   ☐ Username and password

   ☐ Identity number

   ☐ Swipe card

   Guest access

   ☐ Allow guest/anonymous access

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

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. **Note:** You may use the config key: **ext-device.ricoh.soft-keyboard.username.optimize-for-email-address.** For more information, see 4.12 Config Editor.
Identity number	With this option, users use their ID number. For more information, see the PaperCut MF manual. **Note:** If you select this option, you may use the config key: **ext-device.ricoh.use-numeric-input-for-id.** For more information, see 4.12 Config Editor. - **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 required, 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 4.12 Config Editor.
Allow guest/anonymous access	With this option, you may choose to activate **guest** or **anonymous access**, enabling users to be authenticated as a guest user or an anonymous user, 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 a guest user or an anonymous user on the device. • **Guest access** - Selecting **Allow guest/anonymous access** *and also* selecting one or more of the other options (Username and password, Identity number, Swipe card), activates **Guest access**. With this option: ○ A **Guest** button, which may be customized, is displayed on the PaperCut MF Login screen on the device, together with the other 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.ricoh.guest-access.label.** For more information, see 4.12 Config Editor. ○ 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 **Allow guest/anonymous access** *without* selecting any other option, activates **Anonymous access**. With this option:

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

4.3.1 Device's Adaptable Authentication API (AAA)

Using the device's Adaptable Authentication API (AAA), PaperCut MF provides the following details about every logged-in user to other AAA-capable applications on the device (such as, GlobalScan NX 2.4.2 or above):

Field	Description
User.AUTHENTICATOR	The name of the authenticator (PaperCutAaaProvider).
User.AUTHENTICATOR_PROVIDER	The company that created the authenticator (PaperCut).
User.IDENTIFIER; Credential.USER_ID	The user's username.
User.DISPLAY_NAME	The user's full name (if available).
User.EMAIL	The user's email address (if available).
User.HOME_FOLDER	The user's home folder (if available).
Credential.PASSWORD	The user's password. This is only provided if the user entered it during the authentication process. It is only cached for the duration of the user session.

To configure PaperCut MF to provide this information, ensure the config key **ext-device.ricoh.aaa.enabled** is set to **DEFAULT** or **Y**. For more information, see 4.12 Config Editor.

4.4 User authentication via swipe cards

If the **Swipe card** authentication option is selected (see 4.3 User authentication options, 4.4.2 Handling card identifiers), then:

1. Sleep Mode is automatically disabled on the device (see 4.5 Sleep mode).
2. Ensure the card reader is a supported card reader (see 4.4.1 Supported card readers).
3. Access the physical device.
4. Connect the supported card reader (see 4.4.1.1 Connecting supported card readers)
5. Log in to the device as the administrator.
6. Navigate to **User Tools > Screen Features > Screen Device Settings > IC Card Software** Settings.
7. Select **IC Card Reader** > **Proximity Card Reader** or **NFC Card Reader.**
8. Select the required settings for the required card reader.
9. Select **Auth.**
10. Restart the device.

4.4.1 Supported card readers

PaperCut MF – Ricoh (SmartSDK) supports the following configured and compatible card readers:

Manufacturer	Model	Card types
Elatec	TWN4 (various)	CASI-RUSCO / HID / iCLASS / Indala / LEGIC / MIFARE / NexWatch
Inepro	`SCR-708`	EM Microelectronic / HID / iCLASS / Indala / LEGIC / MIFARE
RF IDeas	`MS3-00M1`	Magnetic Stripe
RF IDeas	`RDR-6081`	HID
RF IDeas	`RDR-6381`	Indala
RF IDeas	`RDR-7081`	iCLASS
RF IDeas	`RDR-7581`	iCLASS / LEGIC / MIFARE
RF IDeas	`RDR-80081`	CASI-RUSCO / HID / iCLASS / Indala / LEGIC / MIFARE / NexWatch
RF IDeas	`RDR-80581`	CASI-RUSCO / HID / iCLASS / Indala / LEGIC / MIFARE / NexWatch

4.4.1.1 Connecting supported card readers

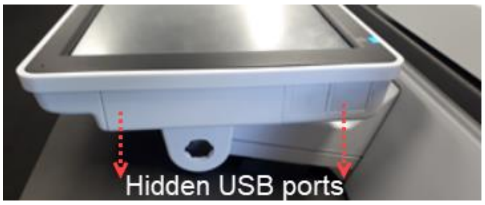
Supported card readers are connected via USB ports on the device. However, the type, availability and location of these USB ports is device-dependent and could be:

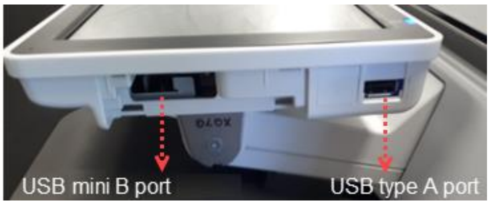
- in a hidden pocket
- covered with a white cap
- visible on the rear panel
- visible on the front panel

While connecting supported card readers:

- only use the USB ports on the device’s front panel.
  Note: USB ports on the device’s rear panel cannot be used to connect card readers.
- if the device has a hidden pocket with USB ports, then it is recommended that you use this. This is because this card reader can be concealed in this hidden pocket, preventing users from attempting to disconnect it in order to access the USB port.
- if the device does not have a hidden pocket but has a covered USB mini B port, then it is recommended that you use this. This is because after the card reader is connected, this port can be covered, preventing users from attempting to disconnect it in order to access the USB

port.





Note: Ensure the device is switched off (powered off) before connecting or disconnecting the card reader.

- if the device does not have a hidden pocket or a covered USB mini B port, then use any other available port on the device's front panel.

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 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 card identifiers using regular expression filters, use the config keys **ext-device.self-association-allowed-card-regex** and **ext-device.card-no-regex**. For more information, see 4.12 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 4.12 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 4.12 Config Editor.

4.5 Sleep mode

Enabling Sleep Mode on a device helps minimize the device's energy consumption. However, when a device enters Sleep Mode, it also powers off any card readers that are connected to the device. This prevents card swipes from waking the panel. Users may need to wake the panel by touching it before attempting to log in with their swipe cards. Some card readers may also require a few seconds to initialize after powering on. This occurs each time the panel wakes from Sleep Mode. As a result, if a device is enabled with swipe card authentication, then Sleep Mode is automatically disabled on the device (the config key **ext-device.ricoh.card-reader.allow-sleep** is set to **N)**.

To toggle Sleep Mode on a device, use the config key **ext-device.ricoh.card-reader.allow-sleep**. For more information, see 4.12 Config Editor.

4.6 SNMP

You must configure the device and PaperCut MF to use SNMPv1/v2c or SNMPv3.

While the device uses SNMP for ICE print jobs, PaperCut MF uses SNMP to:

- block the release of jobs to the device when it is in error, and
- retrieve the device's printer toner levels.

For more information about SNMP, see the PaperCut MF manual.

To configure the device to use SNMP, ensure the **community name** is the same as the value of the config key **ext-device.ricoh.snmp-community** (see 4.12 Config Editor).

To configure PaperCut MF to use SNMP:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In the **External Device Settings,** to enable PaperCut MF to use:
   - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox is not selected (default).
   - SNMPv3, select the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox; and enter the following fields:
     - **Context name** – Enter GWNCS.
     - **Username, Privacy password, Authentication password** - If these values are available at the device's web interface, then use the same values. It not, leave them blank or enter your own value.
     - **Authentication protocol** – Select either **MD5** or **SHA**.
     - **Privacy protocol** – Select either **DES** or **AES**.
5. Click **Apply**.

4.7 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 required 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 required Hold/Release queue. For more information, see the PaperCut MF manual.
   Note: Ensure this does not contradict the settings configured on the device or the device’s web interface. If there is a contradiction, the PaperCut MF Admin web interface settings are overridden and ignored. For more information, see:
   - 2.4.1.3 Configure the device’s user access permission settings
   - 2.4.1.4 Install the PaperCut MF embedded application
   - 2.4.2.2 Configure the device’s administrator access permission settings
   - 2.4.2.3 Configure the device’s user access permission settings
   - 2.4.2.4 Configure the first part of the device’s usage control settings
   - 2.4.2.10 Configure the second part of the device’s usage control settings
   - 6.7 Disabling PaperCut MF from tracking and controlling device jobs

4.7.1 User selection of an account

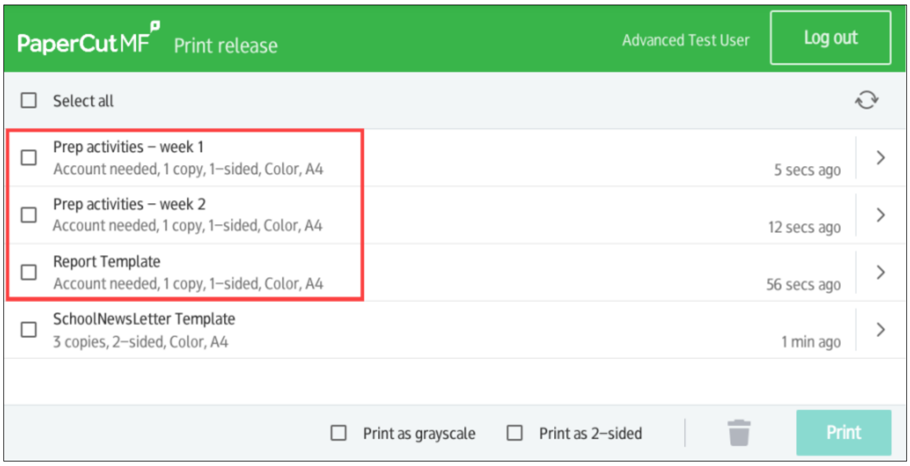
All print jobs must be allocated to an account before they can be released (printed). This account can be either:

- 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:



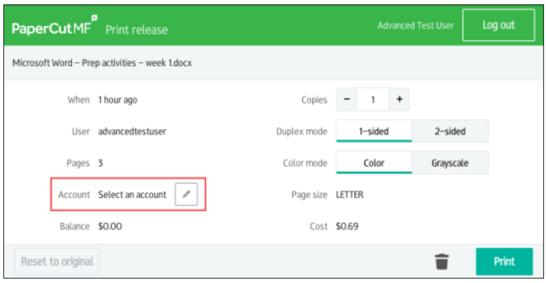
☐ Prep activities – week 1
Account needed, 1 copy, 1–sided, Color, A4 5 secs ago

☐ Prep activities – week 2
Account needed, 1 copy, 1–sided, Color, A4 12 secs ago

☐ Report Template
Account needed, 1 copy, 1–sided, Color, A4 56 secs ago

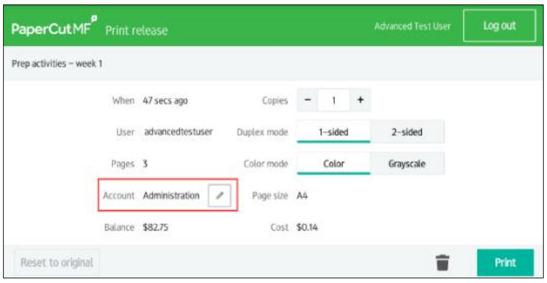
☐ SchoolNewsLetter Template
3 copies, 2–sided, Color, A4 1 min ago

- allocate an account to a *single* held print job without an account or change a previously allocated account:



Microsoft Word – Prep activities – week 1.docx

When 1 hour ago
User advancedtestuser
Pages 3
Account Select an account
Balance $0.00
Copies 1
Duplex mode 1–sided
Color mode Color
Page size LETTER
Cost $0.69



Prep activities – week 1

When 47 secs ago
User advancedtestuser
Pages 3
Account Administration
Balance $82.75
Copies 1
Duplex mode 1–sided
Color mode Color
Page size A4
Cost $0.14

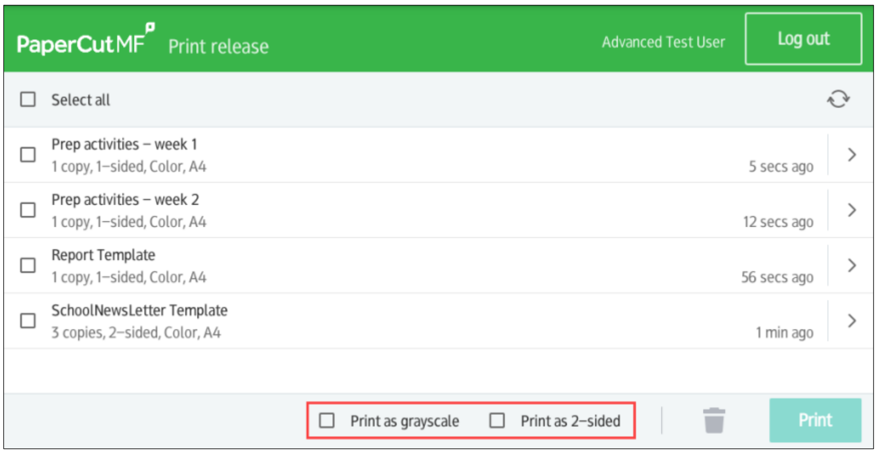
Note: By default, PaperCut MF allows users to select accounts at the device. However, you also have the option of disabling this. For more information, see the PaperCut MF manual.

4.7.2 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)



☐ Prep activities – week 1
1 copy, 1–sided, Color, A4 5 secs ago

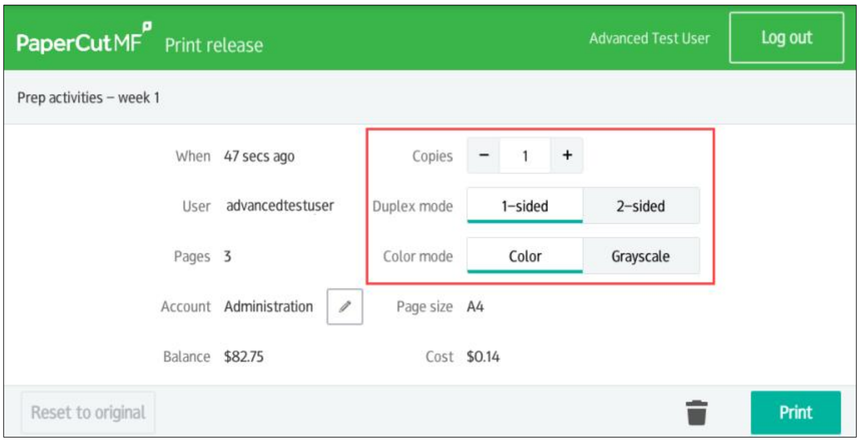
☐ Prep activities – week 2
1 copy, 1–sided, Color, A4 12 secs ago

☐ Report Template
1 copy, 1–sided, Color, A4 56 secs ago

☐ SchoolNewsLetter Template
3 copies, 2–sided, Color, A4 1 min ago

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)



Prep activities – week 1

When 47 secs ago
User advancedtestuser
Pages 3
Account Administration
Balance $82.75
Copies 1
Duplex mode 1-sided
Color mode Color
Page size A4
Cost $0.14

To toggle the display of the cost of held print jobs on the PaperCut MF Print Release screens on the device, use the config key **ext-device.ricoh.release-show-cost**. For more information, see 4.12 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.

4.8 Device jobs

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

4.8.1 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 required device.
4. In the **External Device Settings** area, select the required 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
      Note: This is only applicable to multi-function devices.
    - **Track & control faxing** – PaperCut MF tracks and controls fax jobs
      Note: This is only applicable to multi-function devices.

   Note: Ensure this does not contradict the settings configured on the device or the device's web interface. If there is a contradiction, the PaperCut MF Admin web interface settings are overridden and ignored. For more information, see:
    - 2.4.1.3 Configure the device's user access permission settings
    - 2.4.1.4 Install the PaperCut MF embedded application
    - 2.4.2.2 Configure the device's administrator access permission settings
    - 2.4.2.3 Configure the device's user access permission settings
    - 2.4.2.4 Configure the first part of the device's usage control settings
    - 2.4.2.10 Configure the second part of the device's usage control settings

  - 6.7 Disabling PaperCut MF from tracking and controlling device jobs

4.8.1.1 Device’s ICE print jobs

To configure PaperCut MF to track the device’s ICE (Integrated Cloud Environment) print jobs, ensure:

1. the PaperCut MF Application Server’s system time and time zone are in sync with that of the Cloud server, using the Network Time Protocol (NTP).
2. the device and the PaperCut MF Application Server are configured to use SNMPv1/v2c or SNMPv3. For more information, see 4.6 SNMP.
3. the following config keys are configured as required:
    a. ext-device.ricoh.ice.log-jobs
    b. ext-device.ricoh.snmp-community
    c. ext-device.ricoh.ice.unknown-username
    d. ext-device.ricoh.ice.jobs.incomplete-list
    e. ext-device.ricoh.ice.jobs.timestamp

   For more information, see 4.12 Config Editor

Note: Although PaperCut MF can be configured to track the device’s ICE print jobs, it has some limitations. For more information, see 5.5 Limitations with tracking the device’s ICE print jobs.

4.8.2 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**).
  If the PaperCut MF Account Confirmation screen is displayed, you may also use the config key **ext-device.ricoh.account-confirm.auto-switch.seconds.** For more information, see 4.12 Config Editor.
- To specify the type of soft keyboard displayed on the PaperCut MF Account Selection screen for entering account codes, use the config key **ext-device.ricoh.use-numeric-input-for-account-code**. For more information, see 4.12 Config Editor

4.8.3 Job costs and account balances (Zero Stop)

When printing, if a restricted user’s account balance is insufficient to cover the cost of the restricted user’s entire print job, PaperCut MF prevents the user from being able to start the print job. This ensures that the restricted user’s balance never drops below zero for print jobs.

When scanning, copying, faxing, or on-device printing, PaperCut MF calculates the cost of a single page (i.e. the Reference Page Cost, which is based on configured values). Using this Reference Page

Cost, PaperCut MF calculates the number of reference pages that the restricted user's account balance will allow (i.e. the maximum number of Reference Pages Allowed). As a result:

- If restricted user's account balance is insufficient for even one Reference Page Allowed, then PaperCut MF prevents the user from being able to start a scan, copy, fax, or on-device print job.
- If restricted user's account balance is sufficient for at least one Reference Page Allowed, then PaperCut MF allows the user to start a scan, copy, fax, or on-device print.
  As the job is in progress, if the maximum number of Reference Pages Allowed is reached, then PaperCut MF:
  - stops the job,
  - prevents it from being completed, and
  - deletes the job from the device's Job Status screen.

This ensures that the restricted user's account balance never drops below zero for scan, copy, fax, or on-device print jobs. For more information, see 4.8.3.1 Reference Page Cost and maximum number of Reference Pages Allowed.

4.8.3.1 Reference Page Cost and maximum number of Reference Pages Allowed

To configure the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for scan, copy, fax, or on-device print jobs, use the following config keys:

- **ext-device.ricoh.limit-reference.duplex**
- **ext-device.ricoh.limit-reference.paper-size**

For more information, see 4.12 Config Editor.

Note: This Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for scan, copy, fax, or on-device print jobs, has some limitations. For more information, see 5.2 Limitations of the configured Reference Page Cost and maximum number of Reference Pages Allowed.

4.8.4 PaperCut MF's Integrated Scanning

Note: This is only applicable to multi-function devices.

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

1. Configure it 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:
   - device's scanner archive settings, and PDF/A scan settings (see 2.4.2.6 Configure the device's scanner archive settings, 4.8.4.2 Device's PDF/A scan settings)
   - default settings of the config keys:
     - **ext-device.ricoh.scan.prompt.checkbox.checked** (see 4.8.4.1 Integrated scan workflow)
     - **ext-device.ricoh.timeout.scan-prompt-send.secs** (see 4.8.4.1 Integrated scan workflow)
     - **ext-device.ricoh.scan.color.compression-level** (see 4.8.4.3 Standard color PDF and color JPEG scans)
     - **ext-device.ricoh.scan.high-compression-pdf.enabled** (see 4.8.4.4 High-compression color PDF scans)

4.8.4.1 Integrated scan workflow

If Integrated Scanning is enabled, then you can use the config key **ext-device.ricoh.scan.prompt.checkbox.checked** to specify whether the **Prompt for more pages** checkbox on the Scan Details screen and the Scan Settings screen, is checked or unchecked by default (see 4.12 Config Editor):

- A checked **Prompt for more pages** checkbox enables the device to display the Scan more or finish screen, providing users with the ability to add more pages to the current scan job or start new scan jobs retaining the current scan job's settings and account selection attributes. **Note:** To specify the user inactivity timeout on this screen, use the config key **ext-device.ricoh.timeout.scan-prompt-send.secs**. For more information, see 4.12 Config Editor.
- An unchecked **Prompt for more pages** checkbox enables the device to complete the current scan and send it to the user (scan transfer).

4.8.4.2 Device's PDF/A scan settings

Note: Configuring the device to produce PDF/A scans prevents the production of high-compression color PDF scans (see 4.8.4.4 High-compression color PDF scans).

You can configure the device's PDF/A scan settings using any one of the following options:

- To remotely configure the device to produce PDF/A scan files:
  1. Log in to the device's web interface as an administrator.
  2. Navigate to **Device Management > Configuration > Device Settings > System > General Settings.**
  3. In **PDF File Type: PDF/A Fixed,** select **Active.**
- To physically configure the device to produce PDF/A scan files:
  1. Access the physical device.
  2. Log in as an administrator.
  3. Navigate to **User Tools > System Settings > Administrator Tools**.
  4. In **PDF File Type: PDF/A Fixed,** select **Active.**

4.8.4.3 Standard color PDF and color JPEG scans

To control the compression level that PaperCut MF applies to standard color PDF and color JPEG scans, use the config key **ext-device.ricoh.scan.color.compression-level** (see 4.12 Config Editor):

- If the compression level is low, then scan fidelity is preserved, and scan speed is fast. However, the scan file size is large, so scan transfer could be slow.
- If the compression level is high, then the scan file size is small, so scan transfer is fast. However, scan fidelity is reduced, and scan speed is slow.

4.8.4.4 High-compression color PDF scans

Note: PaperCut MF cannot be configured to produce high-compression color PDF scans if the device is configured to produce PDF/A scans (see 4.8.4.2 Device's PDF/A scan settings).

To configure PaperCut MF to produce high-compression color PDF scans, instead of standard color PDF scans, set the config key **ext-device.ricoh.scan.high-compression-pdf.enabled** to **Y**.

To control other attributes of high-compression color PDF scans, use the following config keys:

- **ext-device.ricoh.scan.high-compression-pdf.color.compression-level**: compression level that PaperCut MF applies to high-compression color PDF scans:

    - If the compression level is low, then scan fidelity is preserved, and scan speed is fast. However, the scan file size is large, so scan transfer could be slow.
    - If the compression level is high, then the scan file size is small, so scan transfer is fast. However, scan fidelity is reduced, and scan speed is slow.
- **ext-device.ricoh.scan.high-compression-pdf.color.compression-method**: scan quality of high-compression color PDF scans:
    - If "JPEG" is used, then the scan quality could be poor. However, this is the more widely supported option.
    - If "JPEG2000" is used, then the scan quality could be better. However, this may not be supported.
- **ext-device.ricoh.scan.high-compression-pdf.image-quality-priority**: scan attribute priority (scan quality or scan speed) of high-compression color PDF scans:
    - If scan quality is high, then scan speed could be slow.
    - If scan speed is fast, then scan quality could be low.
- **Note 1:** This is only applicable to color PDF scans and is only applicable if PaperCut MF is configured to produce high-compression color PDF scans, instead of standard color PDF scans (i.e. the config key **ext-device.ricoh.scan.high-compression-pdf.enabled** is set to **Y**). For more information, see 4.12 Config Editor.
- **Note 2:** Starting from PaperCut MF 22.0, scan actions can now have 3 levels of compression via PaperCut's document processing engine: low, medium, high. If you are using the high compression PDF config key above, we advise against using the new compression settings in the scan action editor, to prevent double compression which could degrade the image quality. We recommend either using the device compression from the config key above, or using the scan action's compression from the scan action output settings. Please make sure no other compression setting is enabled natively in the device.

4.8.4.5 File Uploading

Once the pages have finished scanning, there may be a noticeable delay for the user at the MFD's panel before it indicates a scan is complete. During this time the screen will indicate that the file is uploading. The time that uploading will take is influenced by 2 factors; the time the MFD takes to produce and compress the files, and the size of the file and network speed to the PaperCut MF Application Server. The time the MFD takes to produce and compress the files is significantly noticeable when producing a high-compression PDF file.

To reduce the time a scan job takes to complete at the MFD, the embedded application can be configured to upload scan job files in the background. Once the pages have finished scanning, the UI will immediately inform the user that the scan job has completed rather than waiting for the upload to complete.

Background uploading works in SmartSDK version 3.10 and above. Set config key **ext-device.ricoh.scan.upload.async-disabled** to **N** (see 4.12 Config Editor).

Limitations of uploading in background:

- Users will not be notified when an upload from the MFD to the PaperCut MF Application Server fails.

- When a scan job is uploaded in the background, it will be tracked and charged in the job log even if the upload fails. Scan jobs that upload in the foreground will not be tracked and charged if the upload fails.
- If a device is powered off while there are uploads pending or in-progress those scan files will be discarded and not delivered to the user.
- Due to current firmware limitations, when scanning to a high compression PDF file, if any subsequent scan jobs are started and completed during the time that the MFD is producing the file for the first scan job, the subsequent scan jobs will fail silently, and no files will be delivered to the scan destination.

4.9 Language

4.9.1 Device's Language Selection

Ricoh allows users to change the language of PaperCut MF on the device, using the device's **Change Language** application. However, such changes are only applicable if:

- the config key **ext-device.ricoh.locale** is set to DEFAULT (see 4.12 Config Editor), AND
- PaperCut MF's Language Selection has not been configured or has not been used by the user to change the language of PaperCut MF on the device (see 4.9.2 PaperCut MF's Language Selection).

4.9.2 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.*

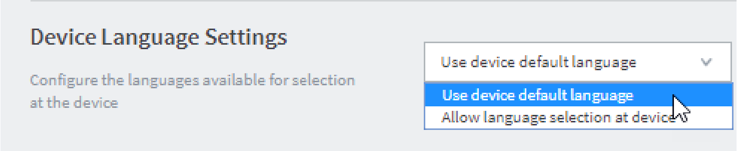
Note: The language selected at the device:

- 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.
- overrides any language changes made using the device's **Change Language** application. For more information, see 4.9.1 Device's Language Selection.
- Maori language selection is supported on Ricoh SmartSDK only.

To configure PaperCut MF's Language Selection:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required 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.ricoh.locale.

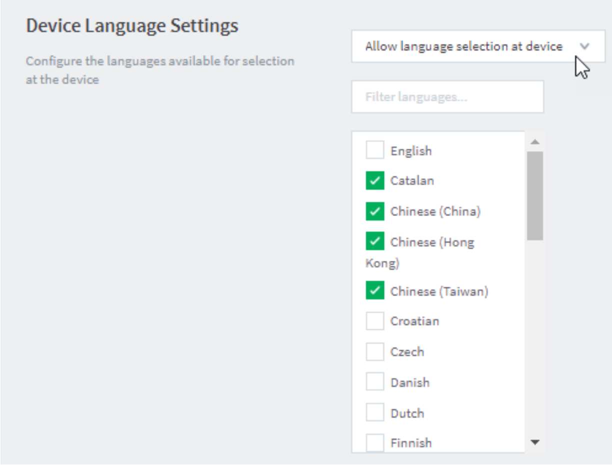


Device Language Settings

Configure the languages available for selection at the device

Use device default language
Use device default language
Allow language selection at device

- **Allow language selection at device**—allow users to select their preferred language via PaperCut MF's Language Selection:



Device Language Settings

Configure the languages available for selection at the device

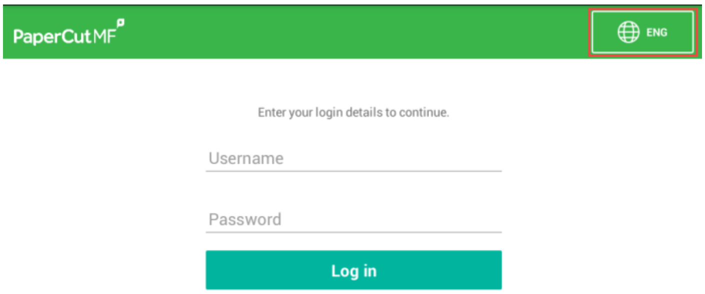
Allow language selection at device

☐ English
☑ Catalan
☑ Chinese (China)
☑ Chinese (Hong Kong)
☑ Chinese (Taiwan)
☐ Croatian
☐ Czech
☐ Danish
☐ Dutch
☐ Finnish

5. If you selected **Allow language selection at device**, select the languages you want to make available for users.
6. Click **OK**.

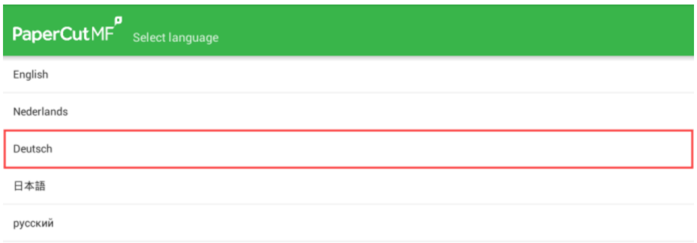
After configuring PaperCut MF's Language Selection, check that it works at the device:

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.ricoh.locale**.

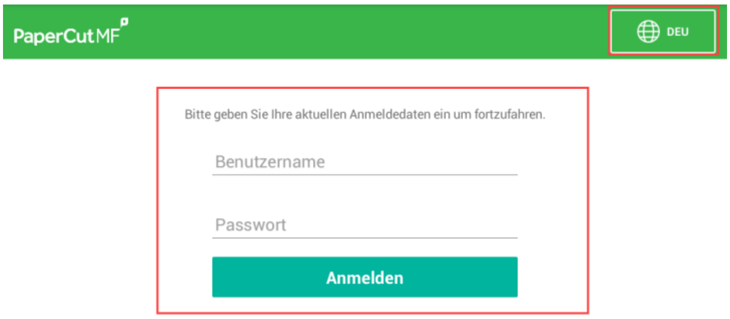


Enter your login details to continue.

2. Select a language.

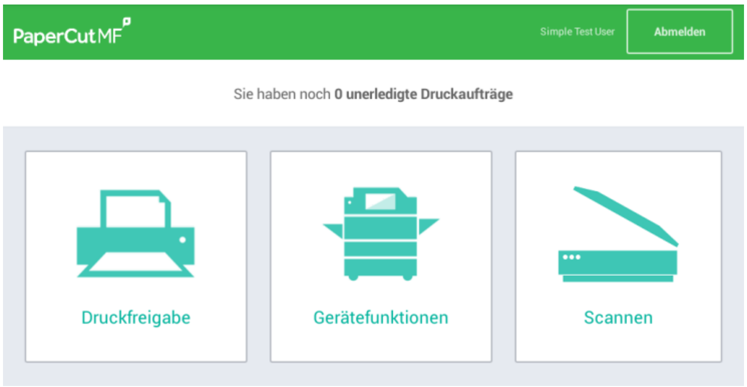


The PaperCut MF Login screen is displayed with the 3-letter language code for the selected language.



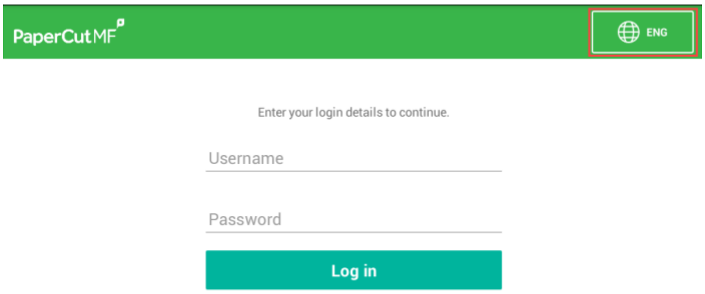
Bitte geben Sie Ihre aktuellen Anmeldedaten ein um fortzufahren.

3. Log in to the device as a test user.
   The text on all the PaperCut MF screens is displayed in the selected language:



Sie haben noch **0 unerledigte Druckaufträge**

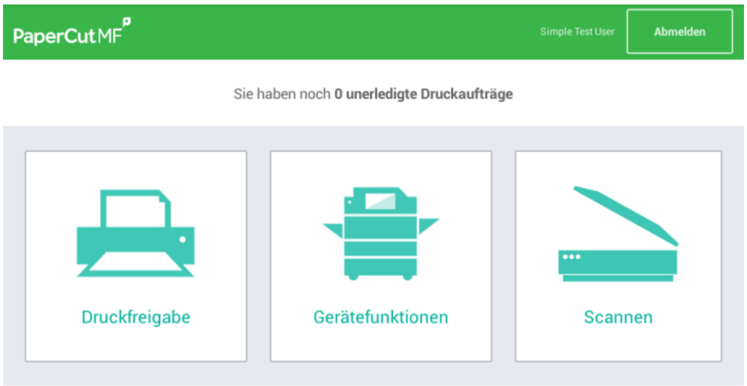
4. Log out of the device.
   The globe button's 3-letter language code reverts to the device's default language ready for the next user.



Enter your login details to continue.

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:



Sie haben noch **0 unerledigte Druckaufträge**

4.10 Colors

To customize the colors of the buttons, images and the header on all PaperCut MF screens:

1. Use the following config keys:
    - **ext-device.ricoh.accent-color**
    - **ext-device.ricoh.primary-color**

   For more information, see 4.12 Config Editor.
2. Log in to the device as a test user (simple test user).
3. Verify that the device's buttons, images and the header colors are as required.

4.11 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 = no more than 55 pixels
    - Image width = no more than 300 pixels
    - Image file size = less than 50 KB
    - Image file format = `.png`
    - Image filename = `logo.png`
    - Image file location = `[PaperCut Install Location]\server\custom\web\device\ricoh-smartsdk\`
2. Log in to the device as a test user (simple test user).
3. Verify that the device's header logo is as required.

4.12 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 configure the device using the available global config keys (impact PaperCut MF on all devices):

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 configure the device using the available device-specific config keys (impact PaperCut MF on the selected device):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Select the required device.
4. Click **Advanced Config.**

The available config keys are:

Config name	Description
Device screens	
ext-device.ricoh.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. ○ prevents language changes made by a user via the device's **Change Language** application from taking effect on PaperCut MF on the device. For more information, see 4.9.1 Device's Language Selection. • 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 4.9.2 PaperCut MF's Language Selection.

ext-device-msg.welcome-text	Customize the text that appears on the PaperCut MF Login screen. For example, instructions to help users log in to PaperCut MF on the device. This is a device-specific config key. • Values: Any text, DEFAULT • Default: DEFAULT (device-specific PaperCut MF text) **Note:** To add a line break, use *\n*. For example, *PaperCut Software\nSwipe your card to log in*.
ext-device.ricoh.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 only applicable if **guest access** is activated (**Allow guest/anonymous access** is selected and at least any one other option is also selected). For more information, see 4.3 User authentication options.
ext-device.ricoh.soft-keyboard.username.optimize-for-email-address	Specify the type of soft keyboard displayed on the PaperCut MF Login screen for entering email addresses during user authentication: • Either, an optimized soft alpha-numeric keyboard (with the "@" and ".com" buttons). • Or, a non-optimized soft alpha-numeric keyboard This is a device-specific config key. • Values: Y (show optimized keyboard), N (show non-optimized keyboard), DEFAULT • Default: DEFAULT (Y) **Note:** • This is only applicable if the **Username and password** authentication option is selected. For more information, see 4.3 User authentication options • Setting this to DEFAULT/ Y – ○ displays the optimized soft alpha-numeric keyboard on all devices, but ○ could make some characters unavailable (such as, the "apostrophe" button).

ext-device.ricoh.use-numeric-input-for-id	Specify the type of soft keyboard displayed on the PaperCut MF Login screen for entering ID numbers during user authentication: • Either, a soft alpha-numeric keyboard • Or, a soft numeric keyboard This is a device-specific config key. • Values: N (show alpha-numeric keyboard), Y (show numeric keyboard), DEFAULT • Default: DEFAULT (N) **Note:** • This is only applicable if the **Identity number** authentication option is selected. For more information, see 4.3 User authentication options • Setting this to Y – ○ displays the soft numeric keyboard, instead of the soft alpha-numeric keyboard on all devices, and ○ is only recommended if the ID numbers of all users only consist of positive integers.
ext-device.ricoh.accent-color	Customize the colors of the buttons, images on all the PaperCut MF screens. This is a device-specific config key. • Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT *(#00b49d)* **Note:** For more information, see 4.10 Colors.
ext-device.ricoh.primary-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 *(#39b54a)* **Note:** For more information, see 4.10 Colors.
ext-device.ricoh.device-functions.label	Customize the text of the **Device functions** icon and the **Use device functions** button that appears on the PaperCut MF Home screen and the PaperCut MF Account Confirmation screen, respectively. This is a device-specific config key.

	• Values: ○ Any text (replaces the defaults on the PaperCut MF Home screen and the PaperCut MF Account Confirmation screen) ○ DEFAULT • Default: DEFAULT (PaperCut MF Home screen: **Device functions**; PaperCut MF Account Confirmation screen: **Use device functions**)
ext-device.ricoh.use-numeric-input-for-account-code	Specify the type of soft keyboard displayed on the PaperCut MF Account Selection screen for entering account codes: • Either, a soft alpha-numeric keyboard • Or, a soft numeric keyboard This is a device-specific config key. • Values: N (show alpha-numeric keyboard), Y (show numeric keyboard), DEFAULT • Default: DEFAULT (N) **Note:** • Setting this to Y – ○ displays the soft numeric keyboard, instead of the soft alpha-numeric keyboard on all devices, and ○ is only recommended if all account codes only consist of positive integers. • For more information, see 4.8.2 User selection of an account.
ext-device.ricoh.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 – ○ hides the account balance, and ○ does not display the savings based on other changes made to held print job settings.

	For more information, see 4.7.2 User selection of job attributes.
ext-device.ricoh.scan.prompt.checkbox.checked	This is only applicable to multi-function devices. Specify the default setting of the PaperCut MF Scan screens' **Prompt for more pages** checkbox (checked or unchecked) and the display of the PaperCut MF Scan more or finish screen (with the three buttons – **Scan more pages, Scan new document, Finish**). 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: N **Note:** For more information, see 4.8.4.1 Integrated scan workflow.
ext-device.ricoh.scan.color.compression-level	This is only applicable to multi-function devices. Specify the compression level applied to standard color PDF and color JPEG scans, when using Integrated Scanning. This is a device-specific config key. • Values: 1 (low compression) – 5 (high compression) • Default: DEFAULT (3) **Note:** For more information, see 4.8.4.3 Standard color PDF and color JPEG scans.
ext-device.ricoh.scan.high-compression-pdf.enabled	This is only applicable to multi-function devices. Specify whether PaperCut MF produces standard color PDFs or high-compression color PDFs, when using Integrated Scanning for PDF scans. This is a device-specific config key. • Values: Y (high-compression PDFs), N (standard PDFs) • Default: DEFAULT (N) **Note:** For more information, see 4.8.4.4 High-compression color PDF scans.

ext-device.ricoh.scan.high-compression-pdf.color.compression-level	This is only applicable to multi-function devices. Specify the compression level that PaperCut MF applies to high-compression color PDF scans, when using Integrated Scanning for PDF scans. This is a device-specific config key. • Values: 1 (low compression), 2 (high compression) • Default: DEFAULT (1) **Note:** This is only applicable if the config key **ext-device.ricoh.scan.high-compression-pdf.enabled** is set to **Y**. For more information, see 4.8.4.4 High-compression color PDF scans.
ext-device.ricoh.scan.high-compression-pdf.color.compression-method	This is only applicable to multi-function devices. Specify the scan quality of high-compression color PDF scans, when using Integrated Scanning for PDF scans. This is a device-specific config key. • Values: JPEG (poor quality), JPEG2000 (better quality) • Default: DEFAULT (JPEG) **Note:** This is only applicable if the config key **ext-device.ricoh.scan.high-compression-pdf.enabled** is set to **Y**. For more information, see 4.8.4.4 High-compression color PDF scans.
ext-device.ricoh.scan.high-compression-pdf.image-quality-priority	This is only applicable to multi-function devices. Specify the scan attribute priority (scan quality or scan speed) of high-compression color PDF scans, when using Integrated Scanning for PDF scans. This is a device-specific config key. • Values: Y (scan quality), N (scan speed) • Default: DEFAULT (N) **Note:** This is only applicable if the config key **ext-device.ricoh.scan.high-compression-pdf.enabled** is set to **Y**. For more information, see 4.8.4.4 High-compression color PDF scans.

ext-device.ricoh.scan.upload.async-disabled	This is only applicable to multi-function devices. Controls whether scan files are uploaded in the background or foreground. See 4.8.4.5 File Uploading This is a device-specific config key. • Values: Y (upload in foreground), N (upload in background if firmware version meets requirements) • Default: DEFAULT (Y)
ext-device.ricoh.scan.upload.concurrent-limit	This is only applicable to multi-function devices. When uploading scan jobs in background, limit the number of uploads that can happen at the same time. Uploads will be queued until the active upload count drops below the limit specified in the config key. This is a device-specific config key. • Values: -1 (no upload limit), Any positive number • Default: DEFAULT (-1)
"Swipe card" authentication option	
ext-device.ricoh.card-reader.allow-sleep	Toggle Sleep Mode on the device. This is a device-specific config key. • Values: N (disable Sleep Mode), Y (enable Sleep Mode), DEFAULT • Default: DEFAULT (N) **Note:** Setting this to Y – is not recommended if the device is enabled with swipe card authentication. For more information, see 4.4 User authentication via swipe cards, 4.5 Sleep mode.
ext-device.card-self-association.use-secondary-card-number	Specify 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 only applicable 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	Specify the regular expression filter to be used to validate card identifiers during card self-association. This is a device-specific config key. • Values: Any valid regular expression, DEFAULT • Default: DEFAULT **Note:** This is only applicable 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.
ext-device.card-no-regex	Specify 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 only applicable 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.card-no-converter	Specify 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 only applicable if the **Swipe card** authentication option is selected. For more information, see 4.3 User authentication options and 4.4.2 Handling card identifiers.
Job costs and account balances (Zero Stop)	
ext-device.ricoh.limit-reference.duplex	When configuring the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for device jobs (such as, scan, copy, fax, on-device printing), specify whether the Reference Page used is a simplex page or a duplex page. This is a device-specific config key. • Values: N (simplex), Y (duplex) • Default: DEFAULT (N) **Note:** For more information, see 4.8.3.1 Reference Page Cost and maximum number of Reference Pages Allowed
ext-device.ricoh.limit-reference.paper-size	When configuring the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for device jobs (such as, scan, copy, fax, on-device printing), specify the paper size of the Reference Page used. This is a device-specific config key. • Values: Any valid paper size, DEFAULT • Default: DEFAULT (Worldwide: A4; North America: Letter) **Note:** For more information, see 4.8.3.1 Reference Page Cost and maximum number of Reference Pages Allowed.
Network resilience, security, debug logs, uninstallation	
system.network-address	Specify the network IP address or FQDN (Fully Qualified Domain 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 FQDN (Fully Qualified Domain 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.ricoh.ice.log-jobs	Specify whether or not PaperCut MF tracks the device's ICE print jobs. This is a device-specific config key. • Values: N (not tracked), Y (tracked) • Default: N **Note:** For more information, see 4.8.1.1 Device's ICE print jobs.
ext-device.ricoh.snmp-community	Specify the community name used when PaperCut MF tracks the device's ICE print jobs. This is a device-specific config key. • Values: Valid name as required • Default: public **Note:** This is only applicable if the config key **ext-device.ricoh.ice.log-jobs** is set to **Y**. For more information, see 4.8.1.1 Device's ICE print jobs.
ext-device.ricoh.ice.unknown-username	Specify the username of the user that is associated with a Ricoh ICE print job if no user was logged in to the device at the time of the job. This is a device-specific config key. **Note:** This is only applicable if the config key **ext-device.ricoh.ice.log-jobs** is set to **Y**. For more information, see 4.8.1.1 Device's ICE print jobs.
ext-device.ricoh.ice.jobs.incomplete-list	This is a device-specific config key that is used internally when PaperCut MF tracks the device's ICE print jobs. **Note:** This is only applicable if the config key **ext-device.ricoh.ice.log-jobs** is set to **Y**. For more information, see 4.8.1.1 Device's ICE print jobs.
ext-device.ricoh.ice.jobs.timestamp	This is a device-specific config key that is used internally when PaperCut MF tracks the device's ICE print jobs. **Note:** This is only applicable if the config key **ext-device.ricoh.ice.log-jobs** is set to **Y**. For more information, see 4.8.1.1 Device's ICE print jobs.

ext-device.block-release-on-error.snmp-error-list	Specify the errors that will prevent jobs from being released. This is a global config key. • Values: DEFAULT, any one or a comma-separated combination of the following printer error types (not case sensitive): o lowPaper o noPaper o lowToner o noToner o doorOpen o jammed o offline o serviceRequested o inputTrayMissing o outputTrayMissing o markerSupplyMissing o outputNearFull o outputFull o inputTrayEmpty o overduePreventMaint • Default: DEFAULT (noPaper, doorOpen, jammed,offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull)
ext-device.ricoh.aaa.enabled	Specify whether or not PaperCut MF provides details about every logged-in user to other AAA-capable applications on the device (such as, GlobalScan NX 2.4.2 or above) using the device’s Adaptable Authentication API (AAA). This is a device-specific config key. • Values: Y, N, DEFAULT • Default: DEFAULT (Y) **Note:** For more information, see 4.3.1 Device’s Adaptable Authentication API (AAA).
Timeouts	
ext-device.ricoh.use-device-functions.timeout.seconds	Specify the interval of time (seconds) that the device waits when attempting to make the required device job

	available to the user, after which it displays an error message. This is a device-specific config key. • Values: Any positive number (seconds) • Default: DEFAULT (30 seconds)
ext-device.ricoh.account-confirm.auto-switch.seconds	Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Account Confirmation screen is automatically taken to the device’s Home screen. This is a device-specific config key. • Values: Any positive integer, DEFAULT • Default: DEFAULT (8 seconds) **Note:** • This is only applicable if the device displays the PaperCut MF Account Confirmation screen. For more information, see 4.8.2 User selection of an account. • Setting this to 0 – disables the auto-switch.
ext-device.ricoh.timeout.scan-prompt-send.secs	This is only applicable to multi-function devices. **PaperCut MF’s Integrated Scanning timeout:** Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan more or finish screen is automatically taken to the PaperCut MF Scan complete (with scan completed or failed status). The process of sending the completed scan job to the user (scan transfer) is also automatically initiated, and the user is logged out. This is a device-specific config key. • Values: Any positive integer, DEFAULT • Default: DEFAULT (30 seconds) **Note:** For more information, see 4.8.4.1 Integrated scan workflow.

5 Known limitations

5.1 Using special characters in usernames

When authenticating a user, PaperCut MF changes some special characters in usernames to other special characters:

- Spaces in usernames are changed to underscores

- Colons in usernames are changed to hyphens
- Double quotation marks in usernames are changed to single quotation marks

For example:

A user with username…	Is authenticated as…
test user	*test_user*
test:user	*test-user*
test"user	*test'user*

As a result, the following is recommended:

- If choosing between underscores and spaces, then only allow any one; not both. If you allow both, then users with identical names, only differing in the special characters used, are both authenticated as the same user. For example:

A user with username…	Is authenticated as…
test_user	*test_user*
test user	

- If choosing between hyphens and colons, then only allow any one; not both. If you allow both options, then users with identical names, only differing in the special characters used, are both authenticated as the same user. For example:

A user with username…	Is authenticated as…
test-user	*test-user*
test:user	

- If choosing between single quotation marks and double quotation marks, then only allow any one; not both. If you allow both options, then users with identical names, only differing in the special characters used, are both authenticated as the same user. For example:

A user with username…	Is authenticated as…
test'user	*test'user*
test"user	

5.2 Limitations of the configured Reference Page Cost and maximum number of Reference Pages Allowed

The Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for scan, copy, fax, or on-device print jobs, has the following limitations.

5.2.1 Limitation 1: Reference Page Cost is lower than the actual per page cost

If the Reference Page Cost is lower than the actual per page cost of the restricted user’s scan, copy, fax, or on-device print job, then the restricted user’s account balance could drop below zero. This is because the cost of the equivalent number of pages of the actual job would be much higher than the cost of the same number of Reference Pages Allowed.

Example 1 – Reference Page Cost is lower than actual job cost

The following is an example of what could happen if the Reference Page Cost is based on an A4 paper size (which costs less than Letter), but the actual job is a Letter paper size. The job is allowed, and the restricted user’s account balance drops below zero.

- **Account’s opening balance** = *$4.50*
- **Attributes and costs of references:**
  - Configured attribute of one Reference Page = A4
  - Calculated cost of one Reference Page = $1.00
  - Maximum number of Reference Pages Allowed = 4
  - Total cost of maximum number of Reference Pages Allowed = $4
  - **Account’s closing balance using References** = *$0.50 (actual job is allowed)*
- **Attributes and costs of actuals:**
  - Attribute of actual page = Letter
  - Cost of actual page = $1.50
  - Number of actual pages = 4
  - Total cost of actual pages = $6
  - **Account’s closing balance using actuals** = *$-1.50 (account balance is negative)*

5.2.2 Limitation 2: Reference Page Cost is higher than the actual per page cost

If the Reference Page Cost is higher than the actual per page cost of the restricted user’s scan, copy, fax, or on-device print job, then even if the restricted user’s account balance has enough funds to cover the actual cost of the job, the following could occur:

- the user could be incorrectly prevented from starting a scan, copy, fax, on-device print,
- the user could be prematurely stopped in the middle of a scan, copy, fax, on-device print.

This is because the cost of the number of Reference Pages Allowed would be higher than the cost of the equivalent number of pages of the actual job.

Example 2 – Reference Page Cost is higher than actual job cost

The following is an example of what could happen if the Reference Page Cost is based on a Letter paper size (which costs more than A4), but the actual job is an A4 paper size. The job is not allowed although the account balance has enough funds to cover the job without dropping below zero.

- **Account’s opening balance** = *$1.50*
- **Attributes and costs of references:**
  - Configured attribute of one Reference Page = Letter

  - Calculated cost of one Reference Page = $2.00
  - Maximum number of Reference Pages Allowed = 0 *(actual job is not allowed)*
- **Attributes and costs of actuals:**
  - Attribute of actual page = A4
  - Cost of actual page = $0.50
  - Number of actual pages = 2
  - Total cost of actual pages = $1.00
  - **Account's closing balance using actuals** = *$0.50 (account balance would not have been negative, if the actual job was allowed)*

5.3 Duplex copy or on-device print jobs with odd number of pages are incorrectly logged

Duplex copy jobs or on-device print jobs with odd number of pages are logged as two jobs on the PaperCut MF Admin web interface (**Logs > Job Log**):

- while all the pages of the copy or on-device print job, except the last odd page, is logged as one duplex copy job,
- the last odd page is logged as another simplex copy job.

For example, a duplex copy or on-device print job of 3 pages is logged as:

- a duplex copy job of two pages, and
- a simplex copy job of one page.

5.4 Scanning portrait pages that don't fit on the glass or the ADF

Note: This is only applicable to multi-function devices.

To scan pages that don't fit on the glass or ADF in portrait mode:

1. Place the pages in landscape mode,
2. Set the **Orientation** scan setting to **Portrait**,
3. If the pages are placed on the glass, then also set the **Duplex mode** scan setting to **1-sided.** This is to avoid every second page from being scanned upside-down.

5.5 Limitations with tracking the device's ICE print jobs

Although PaperCut MF can be configured to track the device's ICE print jobs, it has the following limitations:

- ICE print jobs are logged as copy jobs on the PaperCut MF Admin web interface (**Logs > Job Log**).
- Zero Stop is unavailable; as a result, a restricted user's account balance could drop below zero.
- There is no page-level color detection; as a result, even if there is one color page in an ICE print job, every page of the job is charged at color page rates.

6 FAQ & Troubleshooting

6.1 IP addresses of the PaperCut MF Application Server

To get the IP addresses of the PaperCut MF Application Server, run any one of the following applicable commands from the command line prompt:

- For Windows: `ipconfig`
- For Linux, Mac OS: `ifconfig`

6.2 Ricoh Remote Operation Client (ROC) Status errors

After attempting to initialize the list of devices added on the ROC, if the ROC's Status displays errors, it implies that the details of the devices are incorrect.

To resolve this, ensure that details of the devices are accurate and then resume initializing the list of devices added on the ROC. For more information, see 2.4.1.2 Create the device list and 8 Appendix A: Creating a list of devices on the Ricoh Remote Operation Client (ROC).

6.3 Ricoh Remote Operation Client (ROC) Console errors

After attempting to run the ROC's **Configure for SmartSDK** command, if the ROC's Console displays errors, this could be because the devices that have errored out are:

- Either, unsupported or incompatible with PaperCut's embedded software solution *PaperCut MF – Ricoh (SmartSDK).*
- Or, cannot be configured using the ROC's **Configure for SmartSDK** command.

To resolve this:

1. First, verify if the devices that have errored out are supported and compatible with PaperCut's embedded software solution *PaperCut MF – Ricoh (SmartSDK).* For more information, see 2.1 Supported devices, 2.2 Compatible devices.
2. Then, for the devices that have errored out, attempt to install PaperCut MF without using the ROC. For more information, see 2.4.2 Install PaperCut MF without the Ricoh Remote Operation Client (ROC).

6.4 Device Status "Connecting to server…"

If the **Device Status** displays **Connecting to server…**, it implies that the device is unable to establish connection with the PaperCut MF Application Server. This occurs because of any one of the following reasons:

- There is a network outage that is preventing network connection
- The PaperCut MF Application Server is not running
- The PaperCut MF Application Server's firewall or network routing configuration is preventing network connection
- The details of the PaperCut MF Application Server are incorrect.

To resolve this, ensure the following:

- there is no network outage
- the PaperCut MF Application Server is running
- the PaperCut MF Application Server's firewall or network routing configuration is not preventing network connection

- the PaperCut MF Application Server details are accurate. For more information, see any of the following, as required:
    - 2.4.1.5 Enable communication with the PaperCut MF Application Server or
    - 2.4.2.9 Enable communication with the PaperCut MF Application Server

6.5 PaperCut MF on the device recedes to the background

After PaperCut MF is successfully installed on the device, if the PaperCut MF embedded application comes to the foreground and then recedes into the background, it implies that the **Function Priority** configuration on the device is incorrect.

To resolve this:

1. Log in to the device as an administrator.
2. Navigate to **User Tools > Screen Features > Screen Device Settings**
3. In **Function Priority**, select **PaperCut MF.** For more information, see 2.7 Configure the device's timeout.

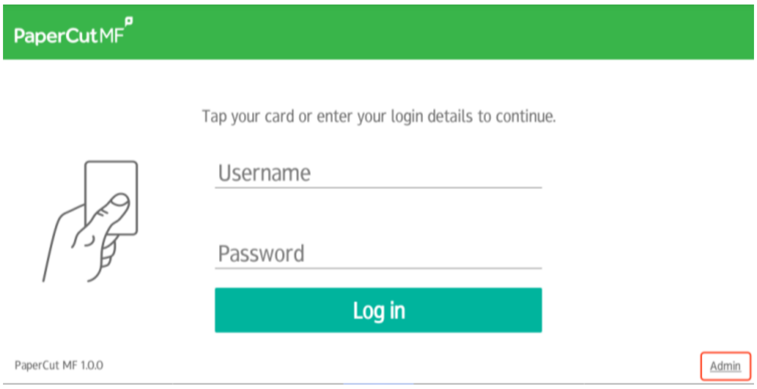
6.6 Accessing administrative jobs

Based on the configured administrative access permission settings, PaperCut MF allows only authenticated administrators to access certain device jobs (such as, administrative jobs).

Note: For more information about configuring the device's access permission settings for required device jobs, see 2.4.2.2 Configure the device's administrator access permission settings.

To access administrative jobs:

1. Access the physical device.
2. Navigate to the PaperCut MF Login screen on the device.
3. Click **Admin**:



Tap your card or enter your login details to continue.

4. Enter the required administrator credentials.

6.7 Disabling PaperCut MF from tracking and controlling device jobs

Depending on the needs of your environment, you can configure the device to disable PaperCut MF from tracking and controlling ***ALL*** or ***SPECIFIC*** device jobs. However, doing so, allows all users, including unauthenticated restricted users with insufficient account balances, to access and use these device job without being charged.

6.7.1 Disabling PaperCut MF from tracking and controlling *ALL* device jobs

To configure the device to disable PaperCut MF from tracking and controlling ***ALL*** device jobs:

- Remotely:

   1. Log in to the device's web interface as an administrator.
   2. Navigate to **Device Management > Configuration > User Authentication Management.**
   3. Select **Off**.

      Note: Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface. If there is a contradiction, the PaperCut MF Admin web interface settings are overridden and ignored. For more information, see 4.7 Secure print release, 4.8.1 Tracking device jobs.

- Physically:
   1. Access the physical device.
   2. Log in as an administrator.
   3. Navigate to **User Tools > System Settings > Administrator Tools > User Authentication Management.**
   4. Select **Off**.

      Note: Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface. If there is a contradiction, the PaperCut MF Admin web interface settings are overridden and ignored. For more information, see 4.7 Secure print release, 4.8.1 Tracking device jobs.

6.7.2 Disabling PaperCut MF from tracking and controlling *SPECIFIC* device jobs

To configure the device to disable PaperCut MF from tracking and controlling ***SPECIFIC*** device jobs:

1. Access the physical device.
2. Log in as an administrator.
3. Navigate to **User Tools > System Settings > Administrator Tools > Application Authentication Management.**
4. Select **Off** for any of the following device jobs as required:
   - *Copier*
   - *Printer*
   - *Document Server*
   - *Fax*
   - *Scanner*

   Note: Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface. If there is a contradiction, the PaperCut MF Admin web interface settings are overridden and ignored. For more information, see 4.7 Secure print release, 4.8.1 Tracking device jobs.

7 Uninstall *PaperCut MF – Ricoh (SmartSDK)*

Depending on your environment and your device, you can permanently uninstall *PaperCut MF – Ricoh (SmartSDK)* using any of the following options:

- 7.1.1 Uninstall PaperCut MF with the Ricoh Remote Operation Client (ROC)
- 7.1.2 Uninstall PaperCut MF without the Ricoh Remote Operation Client (ROC)

7.1.1 Uninstall PaperCut MF with the Ricoh Remote Operation Client (ROC)

To permanently uninstall *PaperCut MF – Ricoh (SmartSDK)* using the ROC:

1. Start the ROC.
2. In the ROC's table, select the required devices.
3. Navigate to **Application > Uninstall.**
4. With the required devices still selected, in **Product ID,** enter **1711276062**; click **Run.**
5. With the required devices still selected, in **Product ID,** enter **33817035**; click **Run.**
   Note: This uninstalls **rxconfServlet.**
6. With the required devices still selected, in **Product ID,** enter **33817044** or **1711276222**; click **Run.**
   Note: This uninstalls **rxspServlet.**
7. With the required devices still selected, navigate to **Application > List apps.**
8. Click **Run**.
9. Verify that the ROC's Console does not display the PaperCut MF embedded application for the required devices.
10. You may need to revisit the required device settings you may have previously configured. For more information, see:
    - 2.4.1.3 Configure the device's user access permission settings
    - 2.4.1.4 Install the PaperCut MF embedded application
    - 2.6 Configure the device's Home screen
    - 2.7 Configure the device's timeout
11. Restart the required devices.
12. Log in to the PaperCut MF Admin web interface.
13. Navigate to **Devices**.
14. Select each required device.
15. Click **Actions > Delete this device**.
16. Click **Devices** and verify that the required devices are no longer listed.
17. Click **Log out**.
18. Access the physical devices.
19. Verify that *PaperCut MF – Ricoh (SmartSDK)* is not available on the required devices.

7.1.2 Uninstall PaperCut MF without the Ricoh Remote Operation Client (ROC)

To permanently uninstall *PaperCut MF – Ricoh (SmartSDK)* without using the ROC:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Device Management > Configuration > Extended Feature Settings > Uninstall.**
3. Select the **PaperCut MF** row; then click **Uninstall**; then click **Ok**.
4. Select the **rxspServlet** row; click **Uninstall**; then click **Ok**.
5. Select the **rxConfServlet** row; then click **Uninstall**; then click **Ok**.
6. You may need to revisit the required device settings you may have previously configured. For more information, see:
   - 2.4.2.1 Configure the device's authentication settings
   - 2.4.2.2 Configure the device's administrator access permission settings
   - 2.4.2.3 Configure the device's user access permission settings
   - 2.4.2.4 Configure the first part of the device's usage control settings
   - 2.4.2.5 Configure the device's user archive settings

   - 2.4.2.6 Configure the device’s scanner archive settings
   - 2.4.2.10 Configure the second part of the device’s usage control settings
   - 2.6 Configure the device’s Home screen
   - 2.7 Configure the device’s timeout
7. Restart the required devices.
8. Log in to the PaperCut MF Admin web interface.
9. Navigate to **Devices**.
10. Select each required device.
11. Click **Actions > Delete this device**.
12. Click **Devices** and verify that the required devices are no longer listed.
13. Click **Log out**.
14. Access the physical devices.
15. Verify that *PaperCut MF – Ricoh (SmartSDK)* is not available on the required devices.

8 Appendix A: Creating a list of devices on the Ricoh Remote Operation Client (ROC)

Note: This is only applicable to:

- post-Spring 2017 devices, or
- pre-Spring 2017 devices, with a Java card installed.

Creating a list of devices on the ROC can be done either:

- via the **devices.csv** file, or
- via the ROC's UI

Based on the option used, ensure that the CSV headers of the **devices.csv** file or the UI fields of the ROC contain valid details as outlined in this table:

CSV header	ROC UI field	Value/ description
IP	**Address**	The IP address or hostname of the device.
Password	**RemoteInstall Password**	The remote installation service password that is specified in the device's web interface (i.e. **Configuration > Administrator Tools > Web Service Settings > Remote Installation Password**).
userwim	**WIM Admin**	The administrator credentials (username) for the device's web interface.
pwdwin	**Password**	The administrator credentials (password) for the device's web interface.
https	**hTTPS**	The communication protocol used by the device to communicate with the ROC. This can be: • *http* • *https* (the device must have SSL enabled) • *https with a fallback to http* (the device must have SSL enabled) If using the **devices.csv** file, this must be any one of the following: • **http** • **https** • **mixed** If using the ROC UI, this must be any one of the following: • *For http* - checkbox is completely unchecked (i.e. blank). • *For https* - checkbox is checked (i.e. ticked)

		• *For fallback* – checkbox is partially checked (i.e. with a dot)
Device Name (SmartSDK)	**Device Name (SmartSDK)**	The unique name for the device. **Note:** The device is registered with this name in the PaperCut MF Admin web interface. If this is blank, then the device is registered with its default name.