PaperCut MF – Xerox LeS Embedded Manual

Contents

1 Document revision history

Published date or release	Details of changes made
22.1.3	Initial version

2 Installation

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

2.1 Requirements

Ensure that the following requirements are satisfied before getting started:

- The PaperCut server software is installed and running on your network. Please see the 'Installation' section of the PaperCut user manual for assistance.
- Ensure that your Xerox device supports eSF version 1.2 or later. Check the device lists in section 2.1.1 below.
- All devices are certified with latest available firmware and hard disk sizes.
- Have available the network name and IP address of the system running PaperCut (e.g. the print server).
- Make sure the network (firewalls, routers etc.) allows TCP connections on ports **9191, 9192** and **9193** from the device to the PaperCut server.
- Ensure that the Xerox device is connected to the network.

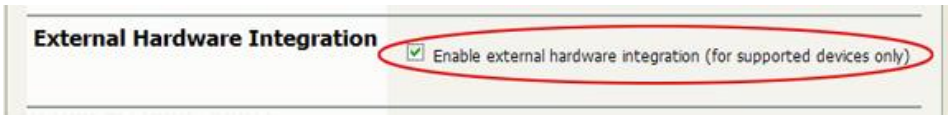
2.1.1 Supported models

Integration is supported for compatible Xerox LeS devices. For a list of supported models, see PaperCut MF for Xerox.

2.2 Setup Procedure

2.2.1 PaperCut Settings

1. Log in to the PaperCut administration interface using a web browser (e.g. http://papercut-server:9191/admin).
2. Navigate to 'Options -> Advanced' and ensure that the option 'Enable external hardware integration' is enabled.



3. Click 'Apply'.

2.2.2 Locating the Embedded Application File

PaperCut offers two versions of the embedded application, targeted at different versions of the embedded services framework (eSF). You must install the version of the application suited to your Xerox device. The following applications are available:

- papercut-les12.fls – for eSF version 1.2 devices
- papercut-les21.fls – for eSF version 2.1+

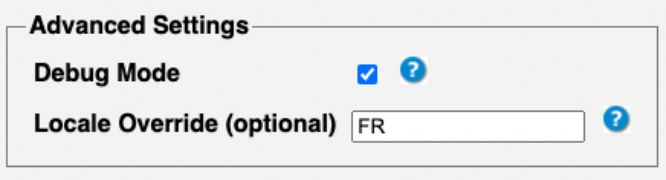
The files are located under your PaperCut installation directory on the server, in the subdirectory `[app-path]/providers/hardware/Xerox`.

2.2.3 Install the PaperCut MF embedded application

Web installation provides a convenient way to install the embedded application. It can be done remotely on multiple devices using just a web browser.
To install the application, perform the following steps:

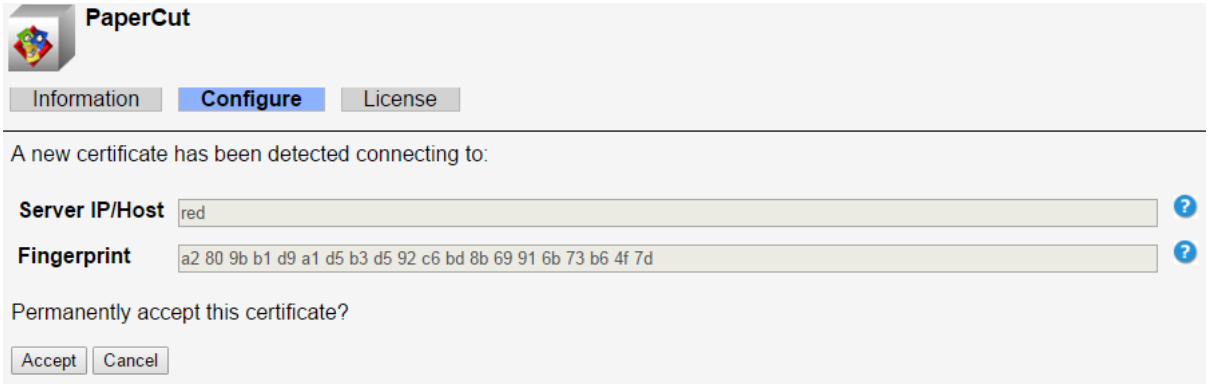
1. Log in to the PaperCut administration interface using a web browser (e.g. http://papercut-server:9191/admin).
2. Navigate to '**Options -> Advanced'** and ensure the **option 'Enable external hardware integration'** is enabled.
3. Press '**Apply'**.
4. Turn on the Xerox device.
5. On a computer, open your web browser
6. Enter the URL of the Xerox device. E.g. http://xerox-device-ip/
7. On devices up to eSF 4.4:
    a. Select the "**Settings**" menu option from the left (also called "**Configuration**" on older devices).
    b. Select "**Embedded Solutions".** On newer devices this is called "**Device Solutions"** instead. Some devices have "**Apps Management**".
    c. If your solution page is called "**Device Solutions",** select "**Solutions (eSF)"** on it. **Do not** select "Additional Solutions".
8. On eSF 5+ devices:
    a. Select the "**Apps**" menu option from the left.
9. Click the **"Install" / "install an app"** / **"Install a New App"** button.
10. Click "**Browse";** then select the appropriate application FLS file.
11. Click "**Start Install" / "Install"**. (On Pre-eSF5 devices) A confirmation message will appear.
12. Click **"Return"** to return to the Embedded Solutions list. The list should now show an item labeled "PaperCut" with "State" indicated as "Running".
13. Click the **"PaperCut**" item.
14. Click **"Configure".**
15. Enter a unique device name (such as "Xerox 1" or "Library Copier") that will later appear in PaperCut MF's list of devices. We recommend adding the placeholder "%SERIALNUMBER%" at any place in the device name to have the device substitute its serial number into the device name. This automatically makes the device name unique and is useful for automated deployments e.g. via Xerox's VSC. Adding the placeholder will be useful later on in case the device's scanner becomes broken or disabled, see FAQ: I see an error: "Device Setup: Duplicate Device name, please see device web interface" after the device has already been successfully created.
16. Enter the PaperCut server's hostname or IP address under "**Server Hostname**". You may need to use the IP address if DNS is not able to resolve the server name correctly.
17. **Optional:** Under "**Advanced Settings",** set the **"Locale Override (optional)"** setting to override the language displayed on the device. This is the 2-letter or 4-letter language code for the required language.

E.g. “FR” or “fr_FR” for French/France. If this is not set-up correctly, an error regarding incorrect locale set may show. See FAQ: I see an unexpected error communicating with server: Unknown locale input section in the FAQ section for more information.



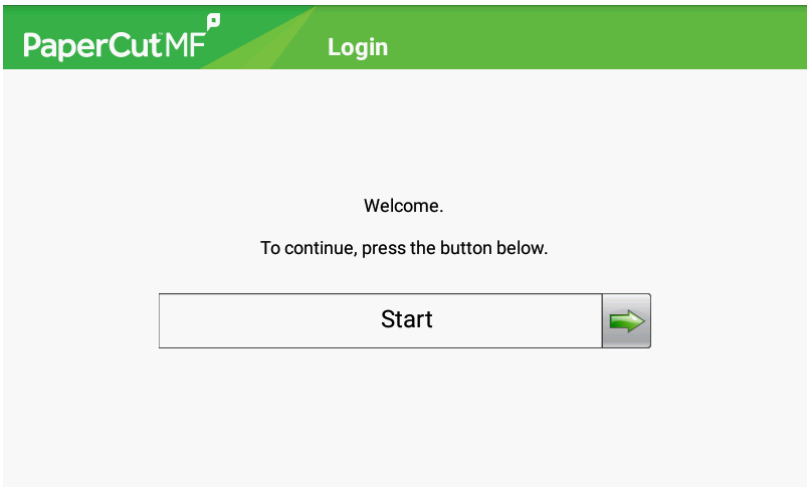
Leave this setting blank if the device’s language is set to “English” and if the country/region is set to an English-speaking region.

18. Leave all other settings at their defaults and click **“Apply”.**
    The device will attempt to connect to the PaperCut server. Once successful, you may need to accept the server's SSL certificate.



    Check that the SHA-1 fingerprint matches the server's certificate. You can also see the certificate details by hovering over the ‘Fingerprint’ question mark (?) icon. See the ‘Troubleshooting SSL’ section of the PaperCut MF manual for details on viewing server certificates.
19. Press the 'Accept' button to permanently accept the server certificate. The device will attempt to connect to the server with the accepted certificate.

20. Once connected, the PaperCut login screen will display on the device.



21. The Xerox device is displayed in the PaperCut Admin web interface under the "**Devices**" tab with the name you provided in the steps above. It will be created using the cost settings of the "[Template Printer]" on the "**Printers**" tab.
22. The embedded application is now successfully installed. To use the photocopier, the users must login to the application, and any copying they perform will be logged in PaperCut.

2.2.4 Configure the device's timeout

2.2.4.1 Login Timeout

When configured, the native device's **Screen Timeout** supersedes PaperCut inactivity timeout (See the config key ext-device.inactivity-timeout-secs in 4.8 Config Editor).

The location of the native device's **Screen Timeout** setting is different for every platform.

- On Gen 5 devices (Android), it can be found in: **Settings > Device > Preferences > Screen Timeout.**
- On Gen4 devices (Non-android), it can be found in: **Settings > General Settings > Timeouts > Screen Timeout.**

While on Android devices, the user is logged out of the device entirely, on non-android devices, the user is only exited from the current screen and returned to the home screen (like the PaperCut inactivity timeout).

2.2.4.2 Logout Timeout

After logging into the device, the device shows the "Home screen", which presents the available functions, such as, copying, scanning, and faxing. This screen is also displayed after the completion of each function.

Note: By default, all non-android Xerox devices, and Android devices with firmware TE363 or above, return to the login screen after a timeout of 5 seconds, requiring the user to go through the login procedure again.

We recommend setting this timeout to 10 seconds, respecting the following considerations:

- On one hand, the timeout should be long enough to provide the user with time to contemplate whether to continue using the device and which function to select.
- On the other hand, the timeout should be short enough to prevent "tailgating", i.e. after a user walks away from the device another user should not be able to walk up to it and continue using it with the previous user's login credentials.

To set the timeout to a different value on an eSF version 1.2 device:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. On the left-hand menu bar, select **"Configuration".**
3. Select **"Security"**.
4. Under **"Auto 'Log out' delay"**, enter a new value, such as, "10"; then click **"Submit"**.

To set the timeout to a different value on an eSF version 2.1+ device:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. Select **"Settings"** on the left-hand menu bar.
3. Select **"General Settings"** under **"Default Settings"**.
4. Select **"Timeouts".**
5. Change **"Screen Timeout"** to an appropriate value and click "**Submit".** This is the amount of time to wait before returning from PaperCut to the device Home screen.
6. On the left-hand menu bar, select **"Settings"**
7. Select **"Security"** under **"Other Settings".**
8. Select **"Miscellaneous Security Settings".**
9. Select **"Login Restrictions".**
10. Change the **"Panel Login Timeout"** to an appropriate version and click **"Submit"**. This is the amount of time to wait before returning from the device Home screen to the PaperCut login screen.

2.2.5 Configure the device's Held Jobs setting

Xerox devices provide a functionality called **"Held Jobs"** that overlaps with PaperCut's hold/release queues. You should deactivate "Held Jobs" in order to avoid confusion with PaperCut MF's print release functions.

eSF 1.2 devices:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. Select "**Configuration"** on the left-hand menu bar.
3. Select **"Security".**
4. Select **"Function Access".**
5. For **"Held Job Access"**, select **"Disable".**
6. Click **"Submit".**

eSF 2.1 – 4.4 devices:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. On the left-hand menu bar, select **"Settings".**
3. Select "**General Settings".**
4. Select "**Home Screen Customization".**
5. Clear **"Search Held Jobs"** and **"Held Jobs"**.
6. Click **"Submit".**

eSF 5.0+ devices:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. On the left-hand menu bar, select **"Settings".**
3. Select **"Device".**

4. Select **“Home Screen Customization”**
5. Clear **“Job Queue”** and **“Held Jobs**”.
6. Click **“Save”.**

2.2.6 Configure the device’s Security Lock-Down setting

In order to prevent unauthorized users from modifying essential device settings, such as disabling copy accounting, a simple security configuration is recommended.

eSF 1.2 devices:

1. On the left-hand menu bar, select **“Configuration”**.
2. Select **“Security”**.
3. Select **“Create/Change Password”.**
4. Select **“Create Advanced Password”.**
5. Enter your desired admin password; then click **“Submit**”. This will prevent all menus and settings from being accessed.
6. To disable any other features such as FTP, Email, or Fax
    a. Select **“Configuration”**.
    b. Select **“Function Access”.**
    c. Set all options to **“Function Disabled”** except:
        - **“Copy Access”—**set to **“No Authentication Required”**
        - **“Profile Access”**—set to **“No Authentication Required”**

    This will deny users access to any functions other than copying and print release. You can revisit this setup later and re-enable other functions, such as e-mail or fax. If you are uncertain of how to set a particular feature you should deny access by setting it to “**No Authentication Required”, "Require user ID",** or **"Requires User ID and Password".**
    d. Click “**Submit**”.

eSF 2.1 – 4.4 devices:

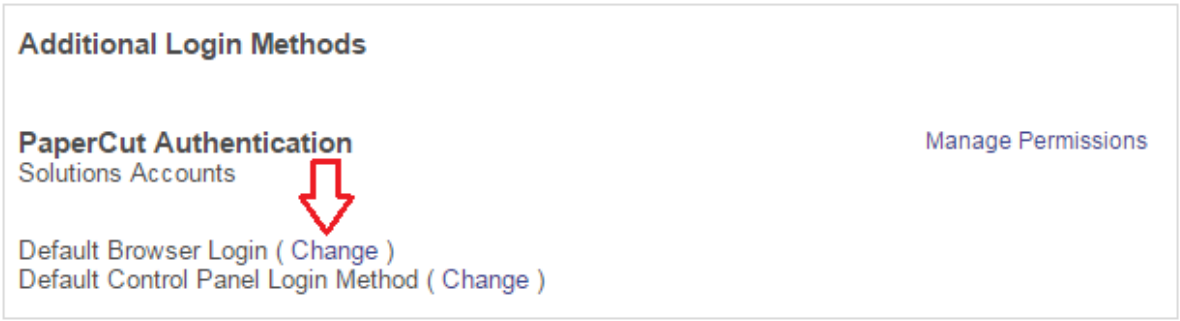
1. Access the Xerox web admin interface under http://xerox-device-ip/
2. On the left-hand menu bar, select “**Settings”.**
3. Under “**Other Settings**”, select “**Security”.**
4. Select **“Edit Security Setups**”.
5. Select **“Password”**.
6. Select “**Add a Password”.**
7. In **“Setup Name**”, enter “**Admin**” and enter the same password twice.
8. Click the “**Admin Password**” checkbox.
9. Click “**Submit**”.
10. Select “**Return to Edit Security Setups**”.
11. Select “**Security Templates”.**
12. Select “**Add a Security Template**”.
13. In “**Security Template Name**”, enter “**Admin**”.
14. From the “**Authentication Setup**”, choose “**Admin**”.
15. Click “**Save Template**”.
16. Click “**Return to Edit Security Setups**”.

17. Select "**Access Controls**".
18. Set **all options** to "**Admin**", or if "**Admin**" is not available, to "**Disabled**" except:
    - "**Operator Panel Lock**"—set to "**Disabled**"
    - "**Copy Function**"—set to "**No Security**"
    - "**Use Profiles**"—set to "**No Security"**

    This will deny users access to any functions other than copying and print release. You can revisit this setup later and re-enable other functions, such as e-mail or fax. If you are uncertain of how to set a particular feature you should deny access by setting it to "**Admin**" or "**Disabled**".
19. Click "**Submit**".

eSF 5.0+ devices:

1. Access the Xerox web admin interface under http://xerox-device-ip/
2. On the left-hand menu bar, select **"Settings"** > "**Security".**
3. Under "**Local Accounts**", click "**Add User**".
4. In "**Name**" and "**User Name**", enter "**Admin**".
5. Enter the same password twice.
6. Click the "**Admin**" checkbox.
7. Click "**Save**".
8. On the "**Security**" menu screen, confirm that "**Additional Login Methods**" lists a single entry titled "**PaperCut Authentication**".
9. On the "**Default Browser Login (Change)**" link, click "**Change**".



10. For "**Control Panel**", select "**PaperCut Authentication**".
11. For "**Browser**", select "**User Name/Password**".
12. Click "**Save**".
13. On the "**Security**" menu screen, under "**Public**", click "**Manage Permissions**".
14. Clear all checkboxes.
15. Click "**Save**".
16. If you were not logged in as an admin, you will need to login now, as the previous step removed administrative access for guests.
    a. On the screen's top-right corner, click "**Log In**".
    b. In "**Login Method**", select "**User Name/Password**".
    c. Enter the admin user name and password (created on step 3).
    d. Click "**Log In**".

17. The default security profile locks access to all but a default set of device functions. You can enable additional functions by configuring the “ext-device.xerox.approved-actions” advanced config key. See 4.8 Config Editor.

2.3 Upgrade the PaperCut MF embedded application on the device

The procedure for upgrading an existing embedded application to a newer version is similar to the initial installation (see section 0 Note: This section covers installation of the PaperCut embedded application for compatible Xerox devices. The embedded application will allow control, logging and monitoring of walk-up off-the-glass copier usage and may serve as a release station for network prints (for information on just tracking network printing see the PaperCut user manual).

2.4 Requirements

Ensure that the following requirements are satisfied before getting started:

- The PaperCut server software is installed and running on your network. Please see the ‘Installation’ section of the PaperCut user manual for assistance.
- Ensure that your Xerox device supports eSF version 1.2 or later. Check the device lists in section 2.1.1 below.
- All devices are certified with latest available firmware and hard disk sizes.
- Have available the network name and IP address of the system running PaperCut (e.g. the print server).
- Make sure the network (firewalls, routers etc.) allows TCP connections on ports **9191, 9192** and **9193** from the device to the PaperCut server.
- Ensure that the Xerox device is connected to the network.

2.4.1 Supported models

Integration is supported for compatible Xerox LeS devices. For a list of supported models, see PaperCut MF for Xerox.

). Please note that only the device-level installation needs to be performed, and you shouldn't have to perform any additional configuration within the PaperCut administrator interface.
After upgrading, it's worth quickly checking the Embedded Application's version number now matches the expected value.

3 Post-install testing

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

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

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

3.1 Test Preparation

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

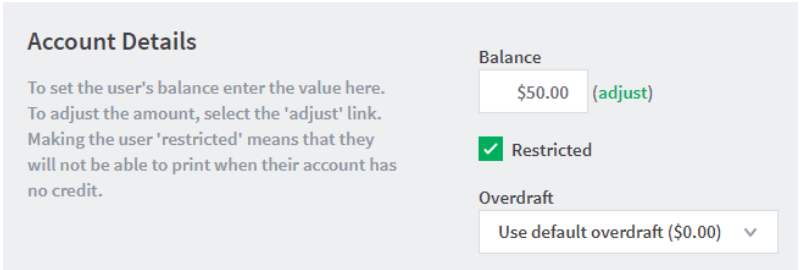
- 'testusersimple' – is used to perform basic copier monitoring and control and to perform print release tests.
- 'testuseradvanced' – is used to perform copier monitoring and control with the account selection enabled (i.e. to charge copying to accounts/departments/cost-centers/etc).

To setup these users in PaperCut:

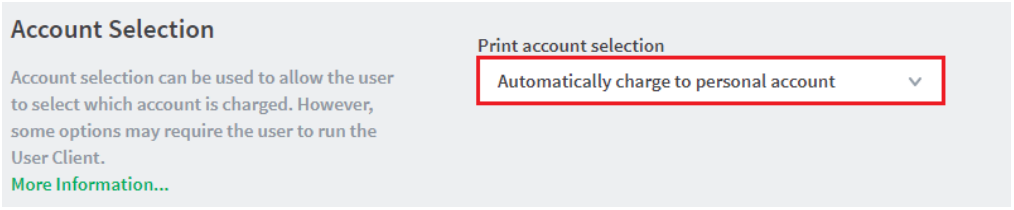
1. Create the 'testusersimple' and 'testuseradvanced' users in your Active Directory or LDAP directory.
2. Login to the PaperCut's admin web interface
3. Go to the "**Options->User/Group sync**" page and press "**Synchronize Now**".
4. Once the sync is complete, the users will be added to PaperCut.

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

1. In PaperCut, select the "**Users**" tab
2. Select the 'testusersimple' user.
3. Set the user's balance to $50.00 and verify the account is set to "**Restricted**".



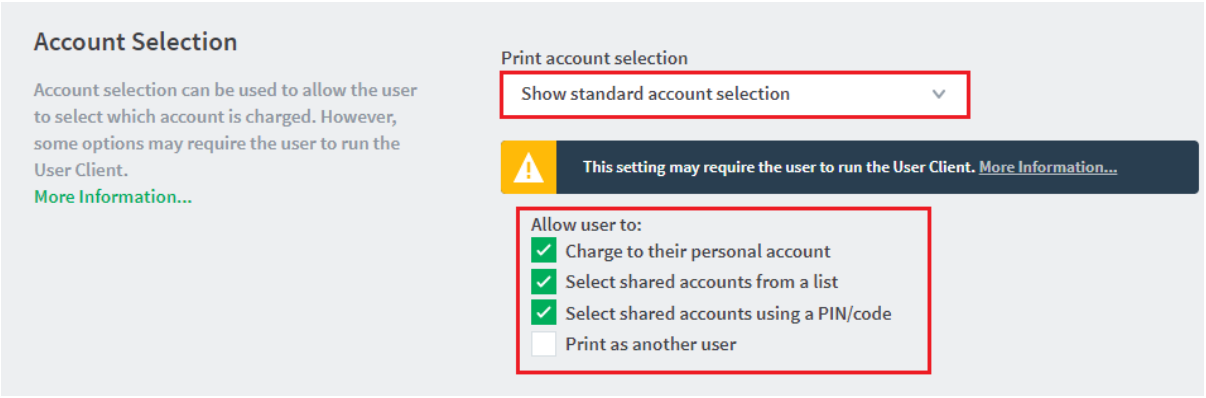
4. Verify that this user is set to "**Automatically charge to personal account**" in the "**Account selection**" options.



5. Press the "**OK**" button to save.

To configure 'testuseradvanced':

1. In PaperCut, select the "**Users**" tab
2. Select the 'testuseradvanced' user.
3. Change the "**Account Selection**" option to "**Show standard account selection**" and enable the relevant account selection options.

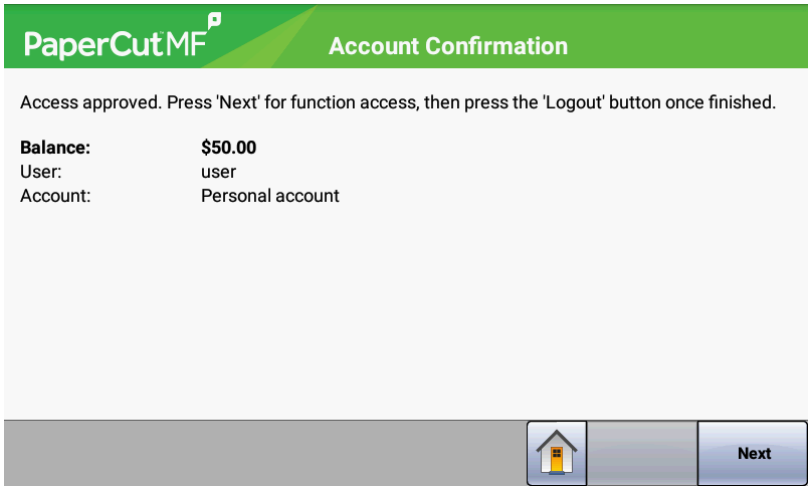


4. Press the "OK" button to save.

3.2 Scenario 1: Standard copying

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

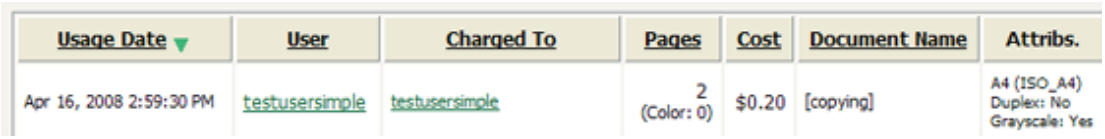
1. At the "**Login**" screen, press "**Start**".
2. Enter the 'testusersimple' username and password.
3. The device will show the home screen with a choice of functions including "**Copy**".
4. Press the "**Copy**" button and perform a copy as normal.



5. Once completed copying the device will return to the home screen.
6. Press the "**Logout**" button.

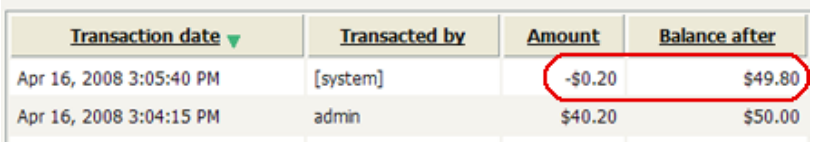
Back in the PaperCut application verify that the copier activity was recorded and that the user's account was deducted.

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



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

4. Click on the user's name in the user column to view the user's account details
5. Select the "**Job Log**" tab to display all print/copy activity for the user.
6. Select the "**Transaction History**" tab and verify that the cost of the photocopying was deducted from the user's account.



Transaction date	Transacted by	Amount	Balance after
Apr 16, 2008 3:05:40 PM	[system]	-$0.20	$49.80
Apr 16, 2008 3:04:15 PM	admin	$40.20	$50.00

3.3 Scenario 2: Copying with account selection

Copying can be allocated to "shared accounts" that represent departments, projects or cost centers. This is commonly used by staff in academic organizations to allocate printing to departments.

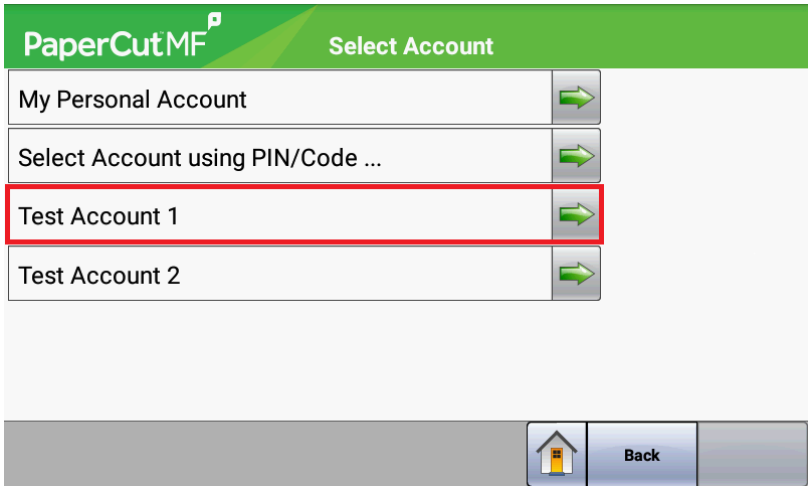
Firstly, some test accounts should be created:

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

6. Press “**OK**”.
7. Repeat the process to create another few accounts.

At the photocopier device:

1. At the “**Login**” screen, press “**Start**”.
2. Enter the ‘testuseradvanced’ username and password.
3. The device will show the home screen with a choice of functions including “**Copy**”.
4. Press the “**Copy**” button. The screen will display the account selection options. Select the account to allocate copying to. E.g. “Test Account 1”.



5. Perform copying as normal. Once completed copying the device will return to the home screen.
6. Press the “**Logout**” button.

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

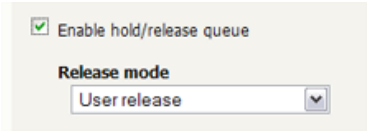
1. Log in to PaperCut
2. Select the device from the “**Devices**” tab
3. Select the “**Job Log**” tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed.
4. Verify the details of the job (i.e. that the job was charged to the selected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

3.4 Scenario 3: Print release

The embedded application may also be used for print release. For a full description of PaperCut hold/release queues and release stations, please read the PaperCut manual. Skip this scenario if hold/release queues will not be used at your site.
To perform print release testing a hold/release queue must be enabled:

1. In PaperCut, select the “**Printers**” tab.
2. Select the print queue (i.e. not the ‘device’) for the Xerox device that will be used for testing.

3. Enable the "**Hold/release queue**" option.



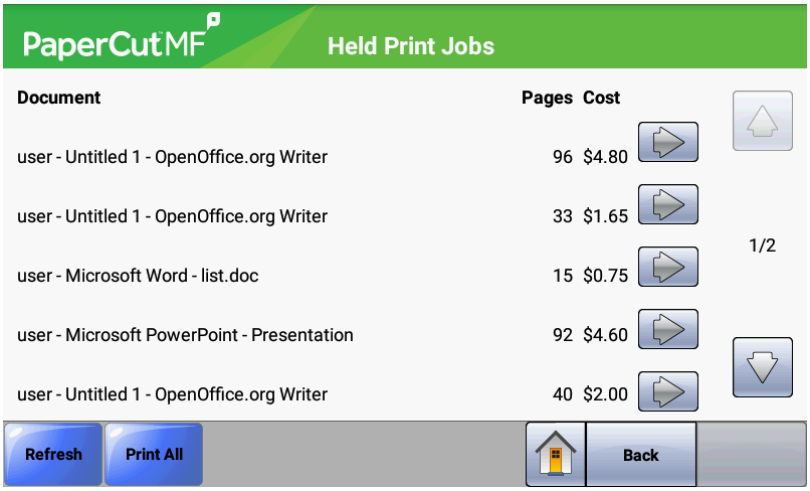
4. Press **OK/Apply** to save the changes. All printing to this queue will now be held until released by a user.

Print Release must also be enabled on the Xerox device:

1. In the PaperCut Admin web interface, select the "**Devices**" tab.
2. Select the required device being tested.
3. In the "**Print Release**" area, select "**Enable print release**".
4. 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.
5. Press "**Apply**" to save.
6. Login to a computer workstation as 'testusersimple'.
7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
8. Confirm that the jobs are held, by checking that the jobs are listed in the "**Printers->Jobs Pending Release**" page of the PaperCut administration interface.
9. Confirm that the username is 'testusersimple'.

At the photocopier device:

1. At the "**Login**" screen, press "**Start**".
2. Enter the 'testusersimple' username and password.
3. The device will show the home screen with a choice of functions including "**Print Release**".
4. Press the "**Print Release**" button.
5. The list of held print jobs is displayed.



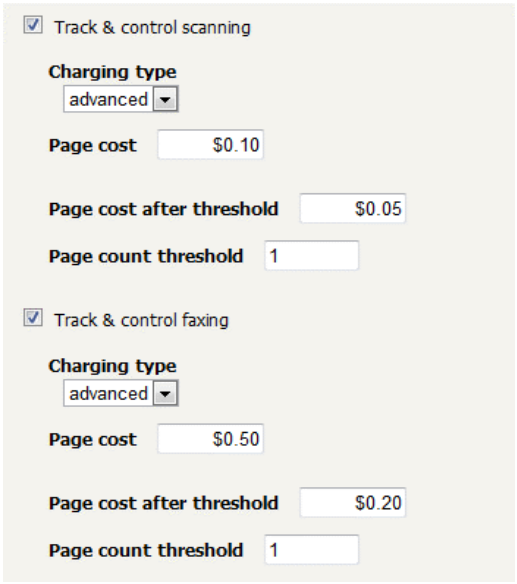
6. Select the job to release by pressing the arrow next to the job.
7. Confirm the release of the print job by pressing the "**Print Job**" button.
8. The job will then print.
9. Try cancelling a job by selecting it and then selecting the "**Cancel Job**" button.

10. The job will be cancelled and will not print.

3.5 Scenario 4: Scanning

Xerox devices can also scan documents and send them by email or to an FTP folder. If a phone line is attached, they can send faxes. You can enable the tracking of scans and faxes. Users can be prevented from scanning or faxing when they are out of credit.
To enable tracking of scans and faxes:

1. In the PaperCut Admin web interface, select the "**Devices**" tab.
2. Select the MFD device.
3. Under "**Device function**" tick "**Track & control scanning**" and "**Track & control faxing**".
4. Select the charging type "advanced" in each case and set some numbers for page costs and thresholds. The cost after the threshold should be lower than the standard cost as it represents a volume discount. As an example, the screen shot below shows that the first page of a scan is charged at $0.10 and any subsequent page at $0.05 whereas the price for faxing is $0.50 for the first page and $0.20 for every page after that.



At the device, log in as 'testusersimple' proceed to do faxing and scanning as usual. Both Scan-to-Email and Scan-to-FTP are supported. Please consult your device manual for details of these operations.
Back in the PaperCut administrator web interface, the job log for the device will show the scan and fax jobs with their respective destinations:

Jun 10, 2010 12:54:08 PM	testusersimple	testusersimple	1	$0.50	[fax] -
Jun 10, 2010 12:50:25 PM	testusersimple	testusersimple	2	$0.15	[scanning] - @papercut.com

Note on sending to multiple destinations:

- When scanning to multiple destinations such as multiple email addresses or multiple FTP folders, the whole scan job is only charged once.
- When sending a fax to multiple phone numbers, each fax sent will be charged separately as a separate fax job.

Note on point-of-charging for faxes: Fax jobs are scanned and then stored by the device for later (asynchronous) faxing. While fax jobs are pending, the red "**Cancel Jobs**" button will display on the device's home screen and can be pressed to inspect the pending jobs and cancel them individually.

- On eSF 2.1+ devices, charging of faxes is delayed until sending over the telephone line has succeeded.
    - This has the benefit that cancelled fax jobs will not be charged.
    - While restricted users' account balance is checked for sufficient credit during the scan process of a fax job, users may in some cases be able to deplete their credit before the fax has completed sending and as such the delayed charging of faxes may result in users overrunning their account balance.
- On eSF 1.2 devices, users are charged at completion of the scan process of a fax job and will not be reimbursed should the fax job subsequently fail to transmit because of a manual cancellation, a busy/faulty telephone number or any other reason.

4 Configuration

After completing the Installation section and registering the device with PaperCut, it will have been configured with default settings that are suitable for most environments. This section covers how to change the default settings.

4.1 Additional Network Security (optional)

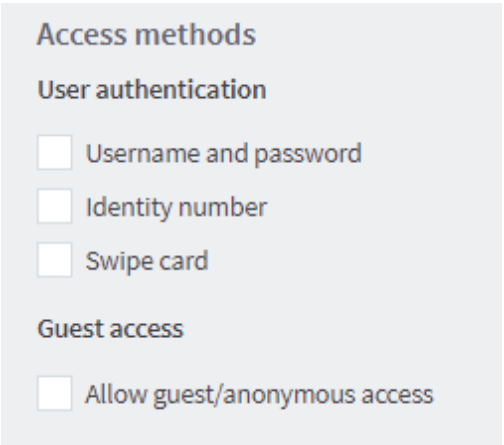
The MFP communicates with the PaperCut server over the network (e.g. to authenticate users or release print jobs). To provide an additional level of security, PaperCut may be configured to only allow device connections from a restricted range of network addresses. This ensures that only approved devices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

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

4.2 User Authentication Options

PaperCut MF provides you with several authentication methods to authenticate users when logging in to PaperCut MF on the device.
To access the available authentication methods on the PaperCut MF Admin web interface:

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



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

The available authentication methods are:

Authentication Method	Description
Username and password	This is the default authentication method. With this method, users use their domain/network username and password.
Identity number	With this method, users use their ID number. For more information, see the PaperCut MF manual. **Require PIN:** With this method, 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 method, 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 method, then see 4.3.1 Supported Card Readers. **Require PIN:** With this method, 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 method, users can use a registered swipe card or a new, unregistered swipe card. If using new, unregistered swipe cards, users are prompted to complete card self-association using their username and password (i.e. associating a new unregistered card with a relevant, valid user account). After card self-association is completed, subsequent use of the registered swipe card does not require users to enter their credentials.
Allow guest/anonymous access	With this method, you may choose to activate **guest** or **anonymous access**, enabling users to be authenticated as guest or anonymous users, as per the user specified in the **Inherit settings from user** field. **Inherit settings from user:** Enter the username of the PaperCut MF user's profile that is used while authenticating users as guest or anonymous users on the device. • **Guest access** - Selecting the **Allow guest/anonymous access** authentication method *and also* selecting one or

more of the other authentication methods (Username and password, Identity number, Swipe card), activates **Guest access**. With this method:

- A **Guest** button, which may be customized, is displayed on the PaperCut MF Login screen on the device, together with the other authentication methods selected.
  Note: You may use the config key **ext-device.xerox.guest-access.label** to customize the text of the **Guest** button that appears on the PaperCut MF Login screen**.** For more information, see 4.8 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.
- Guest users are automatically permitted to access all device functions that are specified in the config keys **ext-device.xerox.approved-actions** and **ext-device.xerox.app-sign-on**. However, you may customize this further to restrict which of the device functions guest users are permitted to access on the device. For more information, see 4.8 Config Editor.

- **Anonymous access** - Only selecting the **Allow guest/anonymous access** authentication method *without* selecting any other authentication method, activates **Anonymous access**. With this method:
  - 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 User Authentication via Swipe Cards

4.3.1 Supported Card Readers

The PaperCut embedded solution for Xerox devices currently supports the following card reader manufacturers:

- MagTek (USB)
- RFIdeas (USB), tested on RDR-67081AKU but may support others
- Elatec, ACID and Weltrend

- OmniKey CardMan 5427, 5321, 5121 and 5125 USB
    - OmniKey readers need a driver that needs to be installed as a separate embedded application alongside PaperCut
    - It is being provided as an *.fls file with a file name such as “omnikeydriver-2.1.2.fls”
    - Please contact your Xerox supplier for the OmniKey driver
    - PaperCut has been tested with the OmniKey driver version 2.1.2

Other keyboard emulating USB card readers may work but should be tested prior to deployment.
Supporting Card Reader authentication is as easy as:

1. Connecting a supported card reader to the device via the USB port (**Note**: On some devices this is hidden under a sticker on the side panel).
2. Enabling ***Swipe card*** as an ***Authentication method*** under the device’s configuration in PaperCut’s web interface.
3. Ensure the card number, as read by the reader, is loaded into the Card Number field in the PaperCut database (or consider using user self-association).

NOTE: Some Xerox devices do not support any form of connected card reader. It is recommended you check with Xerox to confirm support for card readers on your device.

4.3.2 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, converters, or both applied using the PaperCut MF Admin web interface’s **Application Log**.

4.3.2.1 Regular Expression Filters

To extract and validate card identifiers using regular expression filters, use the config keys **ext-device.card-no-regex**, **ext-device.self-association-allowed-card-regex**.
Note: If you customize BOTH the config keys **ext-device.card-no-regex** and **ext-device.self-association-allowed-card-regex**, then you must ensure that:

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

For example:

- if, **ext-device.card-no-regex** = \d{6}(\d{8})
- then, **ext-device.self-association-allowed-card-regex** = \d{8}

For more information, see 4.8 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.

4.3.2.2 Card Number Format Converters

In addition to extracting parts of the card numbers using regular expressions, converting numbers from one format to another is a common requirement. For example, a card reader may report in hexadecimal format, while the number stored in the source (e.g. Active Directory) is in a decimal format. PaperCut includes a number of inbuilt converters to assist here.

Note: Many card readers are configurable - the number format can be changed at the hardware level via utility or configuration tools. PaperCut's software-level converters are there to support card readers that don't offer this level of configuration, or where a global software-level conversion is a better choice. For example, it may be quicker to do the conversion in PaperCut rather than manually reprogram 100+ readers!
Like regexes, the convertors may be defined on either a global (all devices) or on a per-device basis.
To set globally:

1. **Options -> Actions -> Config Editor.**
2. Search for **"ext-device.card-no-converter"**.
3. Enter the name of the required converter (see table below) and click **Update.**

To set at the device level:

1. **Devices -> [select device] -> Advanced Config Editor**.
2. Search for "**ext-device.card-no-converter".**
3. Enter the name of the required converter (see table below) and click **Update.**

4.3.2.3 Standard Format Converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see 4.8 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.	

Tip: Not sure which converter to use? Often trial and error is a good approach. After presenting a card, the number will appear in an application logger message with conversions applied (assuming the card is unknown to the system). Try different converters and inspect the resulting numbers in the application log.

4.3.2.4 Using Custom JavaScript

If the inbuilt converter functions are unable to meet the requirements, it is possible to define your own function using JavaScript. 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 4.8 Config Editor.

4.3.2.5 Other advanced notes

- If *both* a regular expression and a converter are defined, the regular expression is applied first. This means a regular expression can be used to clean up the input (e.g. remove checksum or delimiters) before passing to a converter.
- In some special situations a custom JavaScript implementation may not be enough. For example, there may be a requirement to use a 3rd party system to decrypt the number. PaperCut includes an advanced plugin architecture that the PaperCut Software development team uses to implement these advanced converters. Contact your reseller or Authorized Solution Center to discuss development options and costs. You can find their contact information in your PaperCut Admin interface on the **About** page.

4.4 SNMP

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.

By default, PaperCut MF uses SNMPv1/v2c to perform these actions. You can, however, select to use SMPv3 for better security and encryption.
For more information about SNMP, see the PaperCut MF manual.
To configure PaperCut MF to use SNMP:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In **External Device Settings:**
   - for SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox is not selected (default).
   - for SNMPv3, select the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox; then enter:
     - **Context name, Username, Privacy password**, **Authentication password** – If these values are available at the device web interface, then use the same values. If not, leave them blank or enter your own value.

- **Authentication protocol** – Select either **MD5** or **SHA**.
- **Privacy protocol** – Select either **DES** or **AES**.

Click **Apply**.

4.5 Secure Print Release

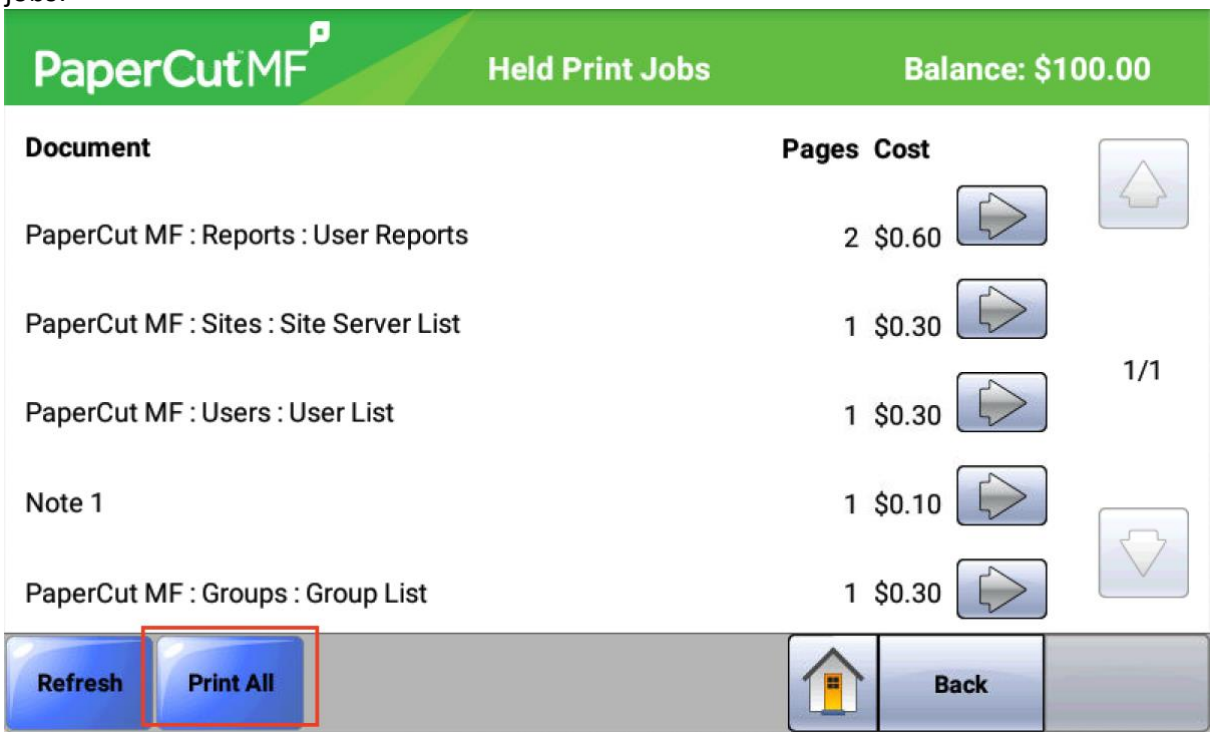
Secure Print Release causes all print jobs to be held at the device until a user releases the job.
To configure Secure Print Release:

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. Under **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.

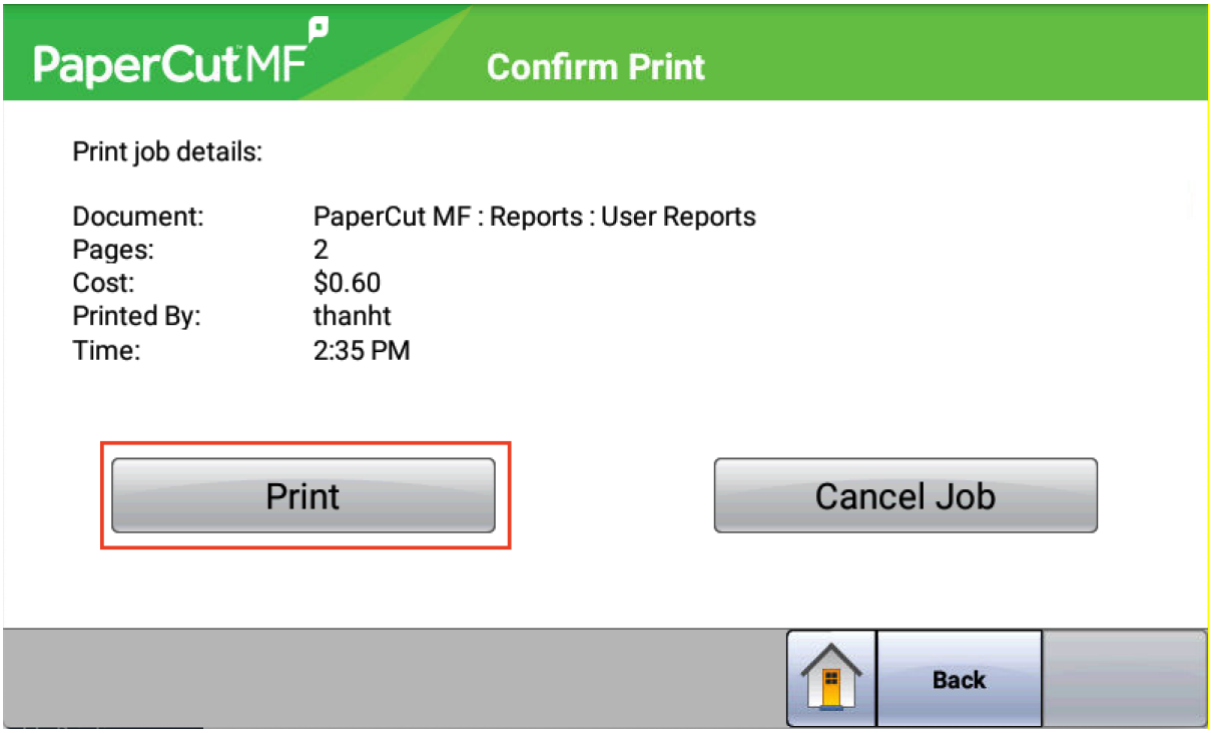
4.5.1 Choose account at the device for printing

All print jobs must be allocated to an account before they can be released (printed). Users can allocate an account to a print job via the User Client and/or at the device (this is only available with PaperCut MF 20.0+, see section 4.7 Account selection at the device).
At the device, users can:

- allocate the same account to all held print jobs without an account and then print all jobs:



- allocate an account to a single held print job without an account and then print the job:



Note:

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

4.5.2 Block the release of jobs to a device in error

If you enable the **"Block the release of jobs when this device is in error" c**heck box in the Admin web interface for a device, you should also hide the warning message displayed when users are releasing documents while the device is still busy printing or copying. This will minimize user confusion, as the message suggests that the user can force the release of jobs, however, if the **"Block the release of jobs when this device is in error"** check box is enabled, they cannot release the job until the error is fixed.
To hide this message:

1. In the PaperCut MF Admin web interface, click "**Devices**".
2. Select a device.
3. Click "**Advanced Config**".
4. Search for "**ext-device.xerox.release.show-busy**".
5. Change the value to "**N**".

Note: This config key is available for devices supporting eSF v2.1 only.

4.6 Device Jobs

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

4.6.1 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:
5. **Track & control copying** – PaperCut MF tracks and controls copy jobs and on-device print jobs
6. **Track & control scanning** – PaperCut MF tracks and controls scan jobs
7. **Track & control faxing** – PaperCut MF tracks and controls fax jobs

If tracked device jobs (scan, copy, fax, on-device printing) are also being charged, then users must allocate them to an account (see section 4.7 Account selection at the device).

4.6.2 Custom Jobs

When the device has a HDD, copying as a Custom Job (job building) is available. PaperCut is unable to ensure that restricted users' account balances do not drop below zero when copying as a Custom Job.
By default, the advanced config key **ext-device.xerox.copy.custom-job.unrestricted** prevents restricted users from copying as a Custom Job (see 4.8 Config Editor). In this configuration, the device itself should also have Custom Jobs disabled, or at least disabled by default.
The native device setting that enables the Custom Job option is called **Allow Custom Job scans**, and you can find it in **Device** or **General settings**. The native device setting that controls the default for Custom Jobs is called **Custom Job scanning**, and you can find it in **Copy settings** (sometimes under **Admin controls**).

4.6.3 Tracking Jobs from Non-Standard Applications

Jobs from non-standard applications are tracked in PaperCut differently to those from standard applications such as "**Copy**", "**Email**", etc. Non-standard applications are those that:

- come preinstalled with some devices, such as "**Forms and Favorites**", "**Scan to Network**" or "**Scan Center"**
- can be installed as eSF applications such as "**Eco Copy**", or
- can be accessed via the "**Profiles**" button on the home screen or through the "**Held Jobs**" menu.

If "**automatically charge to personal account**" or "**automatically charge to single shared account**" are configured for a PaperCut user, non-standard application usage will be automatically charged to the user's personal account or pre-defined shared account, respectively. For any other account selection option, the default is to charge jobs from non-standard applications to the user's personal account.
Jobs from non-standard applications are not subject to credit limits of restricted personal or shared accounts, i.e. users can overrun credit limits by producing jobs through non-standard applications. In environments where enforcing credit limits is desired, it is recommended to disable non-standard applications by removing them from the home screen, via the device's web configuration.
Charging can be configured to display an account selection dialog and charge non-standard application jobs to the selected account instead. Two options are available for non-standard application account selection, each with different limitations:

- Account Selection from Home Screen can be shown when the user selects the non-standard application at the home screen. This is similar to account selection when pressing the buttons for the standard applications, but with the following limitations:
    - The non-standard application needs an "**Access Control**" in the "**Security**" menu of the device's web configuration.
    - Account selection will only be shown once during the session for the selected application and all other non-standard applications. This means that subsequent re-selection of the application from the home screen will not result in the account selection being shown again, nor would selecting another non-standard application. As a consequence, all jobs from non-standard applications will be charged to the selected account until logout.
    - Automatic Sign-On to Applications (see section 4.6.4 Automatic Sign-On to Applications) cannot be activated at the same time.

  To enable Account Selection from Home Screen, configure the access control for each non-standard application with a PaperCut security template (see section 4.6.5 Configuring Application Access Controls with PaperCut Security Templates (eSF 4.4 and earlier devices)). Make sure to configure a different security template (e.g. PaperCut 1, PaperCut 2, etc.) for each application.
- Account Selection at Login can be shown after the user has successfully entered their credentials or swiped their card, with the following limitations:
    - The account selected during login will be used to charge all jobs during the session and no further account selection will be shown until logout. This applies to standard as well as non-standard applications.
    - If print release is enabled, a print release screen will be shown as part of the workflow before the account selection. This is to prevent account selection just to release print jobs, however at least one additional screen press is required to transition from print release to account selection.

  To enable Account Selection at Login, set the advanced configuration property "**ext-device.xerox.login.account-selection**" to "**Y**" (see section 4.8 Config Editor).

4.6.4 Automatic Sign-On to Applications

Copier applications like "**Scan to Network**" and "**Forms and Favorites**" require the user to sign-on to the application using a username and password, even while successfully logged into PaperCut MF. The application uses this second set of credentials to authorize against a network share to deposit scanned documents (Scan to Network) or retrieve documents to print (Forms and Favorites).
Other 3rd party applications (e.g. document workflow applications) require only the username of the authenticated user to direct scanned documents to the correct destination. You can configure PaperCut MF to automatically pass the user's PaperCut MF credentials to the application requiring sign-on, subject to the following limitations:

- PaperCut MF can only pass credentials to one application. E.g. if both "**Scan to Network**" and "**Forms and Favorites**" are present on the copier, one of them has to

be selected for automatic sign-on. All other applications require manual sign-on as before.

- In case the application needs both username and password for its functionality, the user has to log in with a username and password. If the application needs only the username, any login method will work.
- Application sign-on is incompatible with Account Selection from the Home Screen for non-standard applications (see in section 4.6.3 Tracking Jobs from Non-Standard Applications). If account selection for non-standard applications is required with application sign-on, you must enable Account Selection at Login.

To enable automatic sign-on to an application:

- (Only on eSF 4.4 and earlier devices): Configure the application's access control with a PaperCut MF security template (see section 4.6.5 Configuring Application Access Controls with PaperCut Security Templates (eSF 4.4 and earlier devices)).
- (All eSF versions): Change the advanced configuration property "**ext-device.xerox.app-sign-on**" from "**OFF**" to the appropriate access control identifier:

Application	Access Control Identifier
Scan to Network	`esf.scanToNet.scanToNetworkFAC`
Forms and Favorites	`esf.ezForms.ezformsFAC`
Scan Center	`esf.ssa_main.s2aFAC`

- For access control identifiers of other applications, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.
- Some applications can be configured to use the all-purpose numeric access controls "**Solution 1**" to "**Solution 10**". In this case the access control identifier is the number 54 plus the solution number added, e.g. for "**Solution 5**" the identifier is "59".

4.6.5 Configuring Application Access Controls with PaperCut Security Templates (eSF 4.4 and earlier devices)

Account selection for non-standard applications (see section 4.6.3 Tracking Jobs from Non-Standard Applications) and application sign-on (section 4.6.4 Automatic Sign-On to Applications) might require configuring the access control for one or more device applications with a PaperCut MF security template. However, this does not apply to eSF 1.2 devices.

1. Access the device's web interface at http://<device-ip>
2. Navigate to "**Settings > Security > Security Setup**".
3. Under "**Advanced Security Setup**", click "**Security Template**" in "**Step 2**".
4. Click "**Add a Security Template**".
5. In "**Security Template Name**", enter "**PaperCut 1**".
6. From the "**Authentication Setup**" drop-down list, choose "**PaperCut Authentication Module 1**".

7. Click the "**Add Authorization**" button and wait for the page to reappear.
8. From the "**Authorization Setup**" drop-down list, choose "**PaperCut Authentication Module 1**".
9. Click "**Save Template**".
10. Click "**Return to Security Setup**" to return to the main security screen.
11. Click "**Access Controls**" in "**Step 3**".
12. Find the application you would like to configure an access control for in the list.
    - If the list is presented as a list of small yellow folders, it can most likely be found in the "**Device Solutions**" folder.
    - Depending on the device application and its configuration, the corresponding access control might be one of the generic "**Solution 1**" to "**Solution 10**" access controls.
13. From the corresponding drop-down list, choose "**PaperCut 1**".
14. Click "**Submit**".

Repeat this process for every device application that you would like to configure an access control for as per instructions from the previous sections, increasing the number for the security template every time. E.g. for the second application, create a security template named "**PaperCut 2**" with "**PaperCut Authentication Module 2**", then "**PaperCut 3**" with "**PaperCut Authentication Module 3**" etc. A maximum of 5 security templates can be created this way and assigned to a maximum of 5 access controls.
Note: This does not apply to eSF 1.2 devices.

4.6.6 Allowing multiple applications using PaperCut Security Templates access to user data (eSF 4.4 and earlier devices)

By default, user authentication and authorization on eSF 4.4 and earlier devices is handled solely by PaperCut, without the MFD's security subsystem taking part in that process (an exception to this rule is Automatic Sign-On to a specific application, covered in section 4.6.4).
There are cases where the MFD's security subsystem needs to be aware of the user that is currently logged in. One such use-case would be an organization that deploys multiple *Xerox Solution Composer* workflows, each workflow customizing its actions according to the current username.
PaperCut can be configured in such environments to authenticate the user with the MFD's security subsystem as well, making this information available to any 3rd-party apps that query the MFD for this information.
To enable, set the advanced configuration property "**ext-device.xerox.login.perform-auth**" to "**Y**".

4.6.7 Configuring Application Access through the PaperCut MF Application Server (eSF 5.0+ devices)

Starting with eSF 5.0 devices, authorizing users to access the various built-in menus and functions, as well as accessing third-party applications installed on the device is done by PaperCut MF. The list of enabled access controls is configurable through the **ext-device.xerox.approved-actions** advanced device config key. See Config Editor.

4.6.8 Scan Center

Using Scan Center, users can send scan jobs to any of the following based on the authentication method selected:

- 4.6.8.1 Network folders using user credentials
- 4.6.8.2 Network folder using a service account

4.6.8.1 Network folders using user credentials

This is applicable if the authentication method is **Username and password**. For more information, see 4.2 User Authentication Options. To send scan jobs to a network folder using user credentials:

1. Set the config key ***ext-device.xerox.app-sign-on*** to ***esf.ssa_main.s2aFAC.*** For more information, see 4.8 Config Editor.
2. In Scan Center's **Authentication Options** area, select **Use MFP authentication credentials** to create a network folder destination.
3. Either specify the folder address *%homedir%* to send scan jobs to users' home directory network path that is configured while creating and configuring users in PaperCut MF (**Users > User List > User Details > Home directory**), or, specify network's root directory path under which all home folders reside, and in Scan Center's Create Network Folder page, check the Advanced option **Start in User Name Folder**.

4.6.8.2 Network folder using a service account

This is applicable if the authentication method selected is **Identity number** or **Swipe card**. For more information, see 4.2 User Authentication Options. To send scan jobs to a network folder using a service account:

1. In Scan Center's **Authentication Options** area, select **Use static user name and password** to create a network folder destination.
2. Provide all the necessary details (username, password) of the service account.
3. Either specify the folder address *%homedir%* to send scan jobs to users' home directory network path that is configured while creating and configuring users in PaperCut MF (**Users > User List > User Details > Home directory**), or, specify network's root directory path under which all home folders reside, and in Scan Center's Create Network Folder page, check the Advanced option **Start in User Name Folder**.

4.6.9 PaperCut MF's Integrated Scanning

Only applies to eSF 2.1+ and PaperCut MF 20.0+.

To enable users to use PaperCut MF interface to do scanning, use the steps below to initiate 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 default settings of the following config keys:
   - ext-device.xerox.scan.high-compression-pdf.enabled

- ext-device.xerox.scan.prompt.checkbox.checked
- ext-device.xerox.timeout.scan-prompt-send.secs
- ext-device.xerox.timeout.complete-scan-job.secs

For more information, see 4.6.9.1 Integrated scan workflow, 2.2.4 Configure the device's timeout, 4.8 Config Editor.

4.6.9.1 Integrated scan workflow

If Integrated Scanning is enabled, then you can use the config key ext-device.xerox.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 4.8 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 a new scan job 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.xerox.timeout.scan-prompt-send.secs. For more information, see 2.2.4 Configure the device's timeout, 4.8 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).
  Note: To specify the user inactivity timeout on this screen, use the config key ext-device.xerox.timeout.complete-scan-job.secs. For more information, see 2.2.4 Configure the device's timeout, 4.8 Config Editor.

4.7 Account selection at the device

Users may be prompted to select an account when initiating a device job or releasing a print job. This account can be either:

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

Note:

- The options available to users at the device are based on the way users and the device are configured. For more information about configuring cost allocation and shared account access 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**).
- The account search option will only appear if the account list is long. Short lists of only a few accounts will not list a search option.

4.8 Config Editor

The common configuration options for a device in PaperCut are available on the device's **Summary** tab and are discussed in more detail in previous Configuration sections. This

section covers the more advanced or less common configuration options which are available via the **Advanced Config** tab in the device details screen.
The available config keys are:

Config name	Description
Device screens	
ext-device.xerox.header.color	Customize the background color of headers on all PaperCut MF screens. This is a device-specific config key. • Values: #RRGGBB (hexadecimal web/HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT (dark green) **Note:** For more information, see Customizing the Header Logos and Colors
ext-device.xerox.header.textcolor	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 (white) **Note:** For more information, see Customizing the Header Logos and Colors
ext-device.xerox.show-start-prompt	Toggle the display of the welcome screen when there is only one authentication option enabled. This is a device-specific config key. • Values: Y, N • Default: Y **Note:** • Setting this to N – the initial prompt that asks the user to press a button to start logging in will be skipped and the device immediately displays the username or ID number entry prompt. • This is only applicable if **Username and password** access OR **Identity number** access is activated (other

	authentication options and **Allow guest/anonymous access** are disabled).
ext-device-msg.welcome	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.xerox.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 4.2 User Authentication Options.
ext-device.xerox.login.app-only	Instead of showing the PaperCut MF Login screen, defer login to when the user accesses print release, integrated scanning or functions that are being tracked. This is a device-specific config key. • Values: Y, N • Default: N **Note:** • Setting this to Y – the device's home screen is displayed without requiring login.
ext-device.xerox.login.account-selection	**eSF 2.1+ devices only.** Toggle the display of Account selection and/or Print release during the login process. This is a device-specific config key. • Value: Y, N • Default: N. **Note:** See section 4.6.3 Tracking Jobs from Non-Standard Applications for details.

ext-device.xerox.logout.display-icon	**eSF 5.0+ devices only.** Toggle the display of the “Logout” icon that PaperCut adds to the device’s home screen. This is a device-specific config key. • Value: Y, N • Default: Y. **Note:** If set to “N”, the “Logout” icon will not be added. Users are still able to log out by clicking their username on the top-right corner of the device’s home screen.
ext-device.xerox.show-account-confirmation	Toggle the display of Account confirmation after selecting an account. This is a device-specific config key. • Value: Y, N • Default: Y **Note:** • If set to “N”, the message confirming the account selection will be skipped, resulting in a more fluent workflow. • In particular, if account selection is pre-set for all users to their personal or a single shared account and the account is unrestricted the confirmation message is of limited value and should be skipped.
ext-device.xerox.release.document-name.max	**eSF 2.1+ devices only.** Specify the maximum Print Release document name length. This is a device-specific config key. • Value: Any positive number, 0 • Default: 0 (unspecified max length) **Note:** • Some device firmwares are over-conservative with the available screen space available for document names. This setting allows you to override this behavior. • If set to “0”, document names will be displayed on one line, and cut to fit the space. • If set to a positive number, document names will be wrapped to display the maximum length specified. This can result in document names overlapping if you have specified a large maximum length.
ext-device.xerox.release.show-cost	Toggle the display of held print job costs on the PaperCut MF Print Release screens. This is a device-specific config key.

	• Values: Y, N • Default: Y
ext-device.xerox.release.show-busy	**eSF v2.1 devices only.** Toggle the display of the warning message when users are releasing documents while the device is still busy printing or copying. This is a device-specific config key. • Value: Y, N • Default: Y
ext-device-msg.busy-on-release	Specify a message to display when ext-device.xerox.release.show-busy is enabled. This is a device-specific config key. • Value: Any text, DEFAULT • Default: DEFAULT (device-specific PaperCut MF text)
ext-device.xerox.paper-size.default	**eSF 1.2 devices only.** Specify a paper size that will be recorded for a copy job when “AutoSize Match” paper size is selected. This is a device-specific config key. • Value: Any valid paper size • Default: “A4”/”LETTER” depending on country
ext-device.xerox.email.personalized-sender	Specify whether or not the “From” field in the scan-to-email function is pre-filled with the user’s email. This is a device-specific config key. • Value: Y, N • Default: Y **Note:** • Depending on the device model and firmware, “Track and Control Scanning” may have to be enabled.
ext-device.xerox.email.personalized-destination	Specify whether or not the “To” field in the scan-to-email function is pre-filled with the user’s email. This is a device-specific config key. • Value: Y, N • Default: Y **Note:** If set to “Y”, “Track and Control Scanning” is enabled and the email field of the user logged in to the device has been populated in PaperCut, this email address will be set as the “To” field in the scan-to-email function.

ext-device.xerox.email.locked-destination	Specify whether or not the “To” field in the scan-to-email function is read-only. This is a device-specific config key. • Value: Y, N • Default: N **Note:** • If set to “Y” users cannot change the “To” field in the scan-to-email function. • Only use this in conjunction with setting “personalized-destination” to “Y”: Users will only be able to send email to themselves.
ext-device.xerox.scan.prompt.checkbox.checked	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 next page, 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: Y **Note:** For more information, see 4.6.9.1 Integrated scan workflow.
"Swipe card" authentication option	
ext-device-msg.card-association	Specify a message to display when users are requested to associate a swipe card with their user account. This is a device-specific config key. • Value: Any text, DEFAULT • Default: DEFAULT (device-specific PaperCut MF text) **Note:** See section 4.2 User Authentication Options for more information.
ext-device.card-self-association.use-secondary-card-number	Specify the use of the primary or secondary card number field 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 4.2 User Authentication Options
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 4.2 User Authentication Options. • The PaperCut embedded solution for Xerox devices currently supports the following card reader manufacturers: • MagTek (USB) • RFIdeas (USB), tested on RDR-67081AKU but may support others • Elatec, ACID and Weltrend • OmniKey CardMan 5427, 5321, 5121 and 5125 USB ○ OmniKey readers need a driver that needs to be installed as a separate embedded application alongside PaperCut ○ It is being provided as an *.fls file with a file name such as “omnikeydriver-2.1.2.fls” ○ Please contact your Xerox supplier for the OmniKey driver ○ PaperCut has been tested with the OmniKey driver version 2.1.2 Other keyboard emulating USB card readers may work but should be tested prior to deployment. Supporting Card Reader authentication is as easy as:

1. Connecting a supported card reader to the device via the USB port (**Note**: On some devices this is hidden under a sticker on the side panel).
2. Enabling *Swipe card* as an *Authentication method* under the device's configuration in PaperCut's web interface.
3. Ensure the card number, as read by the reader, is loaded into the Card Number field in the PaperCut database (or consider using user self-association).

NOTE: Some Xerox devices do not support any form of connected card reader. It is recommended you check with Xerox to confirm support for card readers on your device.

- Handling Card Identifiers.
- Changing the default value of this config key requires you to ensure that the value of the config key **ext-device.self-association-allowed-card-regex** is only the "extracted, truncated part of the card identifier" of this config key. For example, if the config key **ext-device.card-no-regex** = \d{6}(\d{8}), then the config key **ext-device.self-association-allowed-card-regex** = \d{8}. For more information, see 4.3.2.1 Regular Expression Filters.

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: .* ((dot-star) which includes all card numbers)

Note:

- This is only applicable if the **Swipe card** - **Enable self-association with existing user accounts** authentication option is selected. For more information, see 4.2 User Authentication Options and
- The PaperCut embedded solution for Xerox devices currently supports the following card reader manufacturers:
- MagTek (USB)
- RFIdeas (USB), tested on RDR-67081AKU but may support others
- Elatec, ACID and Weltrend

- OmniKey CardMan 5427, 5321, 5121 and 5125 USB
  - OmniKey readers need a driver that needs to be installed as a separate embedded application alongside PaperCut
  - It is being provided as an *.fls file with a file name such as “omnikeydriver-2.1.2.fls”
  - Please contact your Xerox supplier for the OmniKey driver
  - PaperCut has been tested with the OmniKey driver version 2.1.2

Other keyboard emulating USB card readers may work but should be tested prior to deployment.
Supporting Card Reader authentication is as easy as:

4. Connecting a supported card reader to the device via the USB port (**Note**: On some devices this is hidden under a sticker on the side panel).
5. Enabling *Swipe card* as an *Authentication method* under the device’s configuration in PaperCut’s web interface.
6. Ensure the card number, as read by the reader, is loaded into the Card Number field in the PaperCut database (or consider using user self-association).

NOTE: Some Xerox devices do not support any form of connected card reader. It is recommended you check with Xerox to confirm support for card readers on your device.

- Handling Card Identifiers.
- Changing the default value of the config key **ext-device.card-no-regex** (extracting card identifiers using customized regular expression filters) requires you to ensure that the value of this config key is only the “truncated part of the card identifier” that was extracted by the extraction pattern of **ext-device.card-no-regex**. For example, if the config key **ext-device.card-no-regex** = *\d{6}(\d{8}),* then the config key **ext-device.self-association-allowed-card-regex** = *\d{8}.* For more information, see 4.3.2.1 Regular Expression Filters.

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 4.2 User Authentication Options and
The PaperCut embedded solution for Xerox devices currently supports the following card reader manufacturers:

- MagTek (USB)
- RFIdeas (USB), tested on RDR-67081AKU but may support others
- Elatec, ACID and Weltrend
- OmniKey CardMan 5427, 5321, 5121 and 5125 USB
    - OmniKey readers need a driver that needs to be installed as a separate embedded application alongside PaperCut
    - It is being provided as an *.fls file with a file name such as “omnikeydriver-2.1.2.fls”
    - Please contact your Xerox supplier for the OmniKey driver
    - PaperCut has been tested with the OmniKey driver version 2.1.2

Other keyboard emulating USB card readers may work but should be tested prior to deployment.
Supporting Card Reader authentication is as easy as:

1. Connecting a supported card reader to the device via the USB port (**Note**: On some devices this is hidden under a sticker on the side panel).
2. Enabling *Swipe card* as an *Authentication method* under the device’s configuration in PaperCut’s web interface.
3. Ensure the card number, as read by the reader, is loaded into the Card Number field in the PaperCut database (or consider using user self-association).

	NOTE: Some Xerox devices do not support any form of connected card reader. It is recommended you check with Xerox to confirm support for card readers on your device. Handling Card Identifiers
ext-device.xerox.app-sign-on	**eSF 2.1+ devices only.** Specify an application's access control identifier to automatically sign in to that application with PaperCut credentials. This is a device-specific config key. • Value: an appropriate access control identifier, OFF • Default: OFF **Note:** • See section 4.6.4 Automatic Sign-On to Applications for details. • Customizing this config key for eSF 5.0+ devices, results in being included in the config key ext-device.xerox.approved-actions, automatically permitting access for all users, including guest users. However, if one of the values of the config key ext-device.xerox.approved-actions is *"guest_"* followed by a valid value, then guest users are not permitted to access any device functions specified in this key.
Network resilience, security, debug logs, uninstallation	
ext-device.xerox.login. perform-auth	**eSF 2.1 – 4.4 devices only.** Toggle the use of the MFD's security subsystem at login time to authenticate a user, making the username available for installed 3rd party apps such as Xerox's Solution Composer workflows. This is a device-specific config key. • Values: Y, N • Default: N
ext-device.xerox.approved-actions	**eSF 5.0+ devices only.** Customize which of the device functions users are permitted to access on the device. This is a device-specific config key. Default: • 20 (Grayscale printing from USB drives) • 21 (Color printing from USB drives) • 22 (Scanning to a USB drive)

- 67 (Access address book)
- 84 (Search address book)

Values:

- any one or a comma-separated combination of the following device functions:
  - 0 (Security Menu)
  - 1 (Security Menu Remote)
  - 2 (Se Menu)
  - 3 (Se Menu Remote)
  - 4 (Config Menu)
  - 5 (Diag Menu)
  - 6 (Lock Op Panel)
  - 7 (Change Language)
  - 8 (Supplies Menu)
  - 9 (Supplies Menu Remote)
  - 10 (Paper Menu)
  - 11 (Paper Menu Remote)
  - 12 (Reports Menu)
  - 13 (Reports Menu Remote)
  - 14 (Settings Menu)
  - 15 (Settings Menu Remote)
  - 16 (Network Ports Menu)
  - 17 (Network Ports Menu Remote)
  - 18 (Manage Shortcuts)
  - 19 (Manage shortcuts remote)
  - 20 (Grayscale printing from USB drives)
  - 21 (Color printing from USB drive)
  - 22 (Scanning to a USB drive)
  - 23 (Firmware updates from USB drive)
  - 24 (Import settings from USB drive)
  - 25 (Web import export)
  - 26 (Color Printing)
  - 27 (Copy Function)
  - 28 (Color Copy)
  - 29 (Copy Color Dropout)
  - 30 (Email Function)
  - 31 (Fax Function)
  - 32 (Fax Print)
  - 33 (FTP Function)
  - 34 (Held Jobs)
  - 35 (Profiles)
  - 36 (Shortcuts)
  - 37 (Bookmarks)
  - 38 (Pictbridge Printing)
  - 39 (Thumbprint Printing)
  - 40 (MFP Idle Screen)

- 41 (ESF Config)
- 45 (Disk Wiping)
- 46 (Push Button WIFI Config)
- 47 (Pin WIFI Config)
- 48 (Scan Back)
- 49 (Network Twain)
- 50 (LDD Profiles)
- 51 (LiblexLDAP)
- 52 (Network Se Menu)
- 53 (Remote Management)
- 54 (Firmware Updates)
- 55 (Solution 1)
- 56 (Solution 2)
- 57 (Solution 3)
- 58 (Solution 4)
- 59 (Solution 5)
- 60 (Solution 6)
- 61 (Solution 7)
- 62 (Solution 8)
- 63 (Solution 9)
- 64 (Solution 10)
- 67 (Access address book)
- 68 (Create Profiles)
- 76 (Cancel Jobs)
- 77 (New Solutions)
- 78 (Bundle Import Export)
- 79 (Secure IPP Print)
- 81 (Access to USB Drive)
- 82 (Option Card Menu)
- 83 (Device Menu)
- 84 (Search Address Book)
- 85 (Print Permissions BW)
- 86 (Out of Service and Restore)
- 87 (Network Folder Print)
- 88 (Network Folder Color Printing)
- 89 (Network Folder Scan)
- 90 (Hard Disk Print)
- 91 (Hard Disk Color Printing)
- 92 (Hard Disk Scan)

- 3rd party apps:
  - esf.ssa_main.s2aFAC (Scan Center application)
  - esf.ezForms.ezformsFAC (Forms and Favorites)

	○ esf.cardCopy.cardCopyFAC (Card Copy) ○ esf.googledocs.gdriveFAC (Google Drive Application) • Any of the above character strings, truncated and suffixed with "*" (Device functions that begin with truncated versions of their character strings followed by "*" are accessible to all users. For example, "esf*" allows users to access all device functions that begin with the character string "esf".) • Any of the above values prefixed with "guest_" (Device functions that begin with guest_ are the only device functions that are accessible to guest users. For example, "guest_27" allows guest users to only access device function 27, copying.) **Note:** • The above list includes both user and administrative device functions. It is recommended that user access is permitted only for user device functions and not administrative device functions. • The above list may not be an exhaustive list of all device functions, device capabilities, and third-party applications that may be available on the device. For a complete list, contact your reseller or Authorized Solution Center. • User access, including guest user access, is also automatically permitted for any device function specified in the config key ext-device.xerox.app-sign-on, except if one of the above values contains the prefix "guest_" followed by a valid value.
ext-device.xerox.copy.custom-job.unrestricted	Specify whether or not copying as a Custom Job is allowed for all users (restricted and unrestricted) This is a device-specific config key. • Values: Y, N • Default: N **Note:** • Setting this to Y – ○ allows all users (restricted and unrestricted) to copy as a Custom Job ○ could cause restricted users' account balances to drop below zero. • Setting this to N –

	○ allows only unrestricted users to copy as a Custom Job ○ blocks restricted users from copying as a Custom Job ○ ensures restricted users' account balances do not drop below zero. For more information, see 4.6.2 Custom Jobs.
ext-device.xerox.hold-copies	Toggle the copy option that scans all pages before printing the first page. This is a device-specific config key. • Value: Y, N, DEFAULT • Default: DEFAULT (Y) **Note:** • If set to "N" printing starts as soon as the first page has been scanned. • This option is ignored on devices without a hard disk where printing will always start after the first page. • Set to "DEFAULT" or "Y" for strict zero stop at the cost of a longer wait for the first copied page to be printed. Set to "N" for faster printing of the first copied page.
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): ○ lowPaper ○ noPaper ○ lowToner ○ noToner ○ doorOpen ○ jammed ○ offline ○ serviceRequested ○ inputTrayMissing ○ outputTrayMissing ○ markerSupplyMissing ○ outputNearFull ○ outputFull ○ inputTrayEmpty ○ overduePreventMaint

	• Default: DEFAULT (noPaper, doorOpen, jammed,offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull)
ext-device.xerox.scan.high-compression-pdf.enabled	Specify whether or not PaperCut MF attempts to produce high-compression PDFs (if possible), when using Integrated Scanning. This is a device-specific config key. • Values: Y (high-compression PDFs), N (standard PDFs) • Default: DEFAULT (N) **Note:** This is only applicable to color and grayscale Integrated Scan PDFs; this has no effect on monochrome (black & white) Integrated Scan PDFs or other file types. For more information, see 4.6.9 PaperCut MF's Integrated Scanning.
Timeouts	
ext-device.inactivity-timeout-secs	PaperCut MF timeout: Specify the interval of time (seconds) after which a user who is detected as being idle on PaperCut MF is automatically logged out. This is a device-specific config key. • Values: Any positive number (seconds) • Default: 60 (seconds) **Note:** This only applies when it is lower than the value of the device's screen timeout. For more information, see 2.2.4 Configure the device's timeout.
ext-device.xerox.release.show-busy.job-timeout	Specify the interval of time after which the jobs that have been paused (paper jam, out of paper) are considered not to be keeping the printer busy. This is a device-specific config key. • Value: Any positive integer • Default: 300 **Note:** This only applies when ext-device.xerox.release.show-busy is enabled.
ext-device.xerox.timeout.scan-prompt-send.secs	**PaperCut MF Scan More or Finish 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 (with the three buttons – **Scan next page, Scan new document, Finish**) is automatically taken to the PaperCut

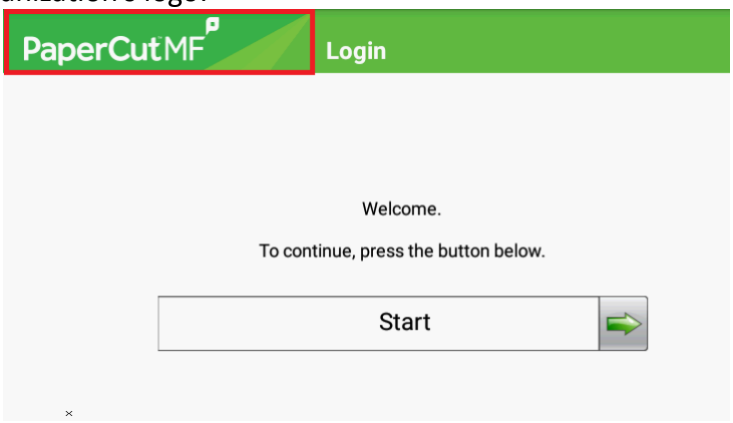
	MF Scan Complete screen (with scan completed status). The user is automatically returned to the home screen. This is a device-specific config key. • Values: 1-300 (seconds) • Default: 30 (seconds) **Note:** This only applies when it is lower than the value of the device's screen timeout. For more information, see 2.2.4 Configure the device's timeout.
ext-device.xerox.timeout.complete-scan-job.secs	**PaperCut MF Scan Complete timeout:** Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Complete screen (with scan completed or failed status), is automatically returned to the home screen. This is a device-specific config key. • Values: 1-300 (seconds) • Default: 5 (seconds) **Note:** This only applies when it is lower than the value of the device's screen timeout. For more information, see 2.2.4 Configure the device's timeout.

4.9 Customizing the Header Logos and Colors

The embedded application has a header at the top of all screens. This header defaults to the PaperCut logo and green color. The header can be customized to match your organization's color scheme and logos.

4.9.1 Customized Logos

The embedded application header has a header logo (as shown below). You can replace this logo with your organization's logo.



This shows the logo outlined in red. The image must be saved as a GIF file with the following filename and size:

- Icon logo: `icon-logo.gif` – 312 x 64 pixels

These images should be saved on the PaperCut application server in the PaperCut application directory under the subdirectory `server\custom\web\device\xerox`. Create the subdirectory if necessary. The embedded application will fetch the images from the server to display them on the device screen.
Minor deviations from the recommended horizontal pixel size are possible for the text logo (wider or narrower). Verify the correct layout on the device screen after producing the image.

4.9.2 Custom Header Color

The header colors are defined in the “Advanced Config” in the devices details screen, see section 4.8 Config Editor. The options to change are:

- ext-device.xerox.header.color – the background color (type DEFAULT for the default setting of dark green)
- ext-device.xerox.header.textcolor – the text color (type DEFAULT for the default setting of white)

The colors are specified using the hexadecimal web/HTML notation (#RRGGBB) where “RR” is the red component, “GG” is the green component and “BB” is the blue component.

4.10 Customizing Text and Messages

PaperCut allows some text that appears in the device to be customized. The custom text might include instructions or terminology that is more appropriate for the site. An example of text that is customizable is the “Welcome text” that displays before the user logs in to the device.
The text can be customized by editing the device configuration from the PaperCut administration interface. For more details, see the 4.8 Config Editor section.

5 Known Limitations and Security

5.1 Known Limitations

On all devices:

- When using the “Auto Match” paper size setting, “Customer Job” mode, separator sheets or booklet printing, the cost of a job cannot be estimated accurately prior to printing. For restricted users, this may result in the job starting to print and getting

stopped before it is complete. It may also result in an account overdraft of a few pages.

- When doing a copy duplexed job, the job may be tracked as a mixed (duplex/simplex) job when there is an odd number of input pages scanned.

The following limitations exist on Xerox eSF 5+ devices:

- Some Xerox devices ship with an optional application called “Scan Center”. This application allows a document to be scanned once and then automatically routes the image to one or more selectable destinations such as email, copier, fax etc.
  Some scan jobs generated through Xerox’s Scan Center as well as other third party applications (such as Shortcuts), cannot be tracked by PaperCut MF, nor can PaperCut MF prevent a user with insufficient balance from performing such jobs. These jobs include faxing using a fax server, scan to email using Scan Center, scan to ftp using Scan Center. If this poses a concern, you can disable some Scan Center connectors (for example, disable 'Scan Center - Printer' to prevent standard copy jobs through Scan Center), or remove the Scan Center app altogether.

The following limitations exist on Xerox eSF 3.1 devices:

- Depending on firmware, copy jobs with an output paper size selection of “Auto Size Match” may not perform zero-stop correctly when the output paper size is not Letter (US/Canada) or A4 (other countries).
  Inquire with Xerox or your reseller or Authorized Solution Center about whether your devices’ firmware supports “Auto Size Match” correctly. You can find their contact information in your PaperCut Admin interface on the **About** page. If not supported, this means that
  - For copy jobs with output paper sizes with a cost lower than the cost of A4/Letter the copy job may be denied with a reason of insufficient credit even when sufficient credit is available.
  - For copy jobs with output paper sizes with a cost higher than the cost of A4/Letter the copy job may result in an account overrun.

The following limitations exist on Xerox eSF 2.1 devices:

- No limitations or issues are known at this time.

The following limitations exist on Xerox eSF 1.2 devices:

- Duplex copies may at times not be charged correctly in mixed duplex/simplex copy jobs such as copy jobs involving multiple copies of a range of pages where ranges of duplex pages are interspersed with the occasional simplex page.
- Copy jobs with an output paper size selection of “Auto Size Match” are not recorded correctly with respect to the output paper size used. The paper size recorded will be the configuration value “ext-device.xerox.paper-size.default” (see section 4.8 Config Editor) irrespective of the actual paper size used.

5.2 Security concerns

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

- The copier's admin password (see section 2.2.6 Configure the device's Security Lock-Down setting) always be kept secure.
- The power and network cable should be securely connected. The system is designed to be robust and record copier usage if the power is lost during copying, but it is possible to start copying before the embedded application starts after restarting the copier.

6 FAQ & Troubleshooting

What is the IP address of my PaperCut Server?
Use operating system command-line tools such as `ipconfig` or `ifconfig` to determine this.

The embedded application shows "Device Setup: Connecting to server …'?
This indicates that the embedded application is unable to connect to the PaperCut server over the network. The embedded application will continually try to connect to the server (trying both the server name and IP), so if there is a temporary network outage then it will start working once the connection is available again.
Common causes of this problem are:

- The PaperCut application server is not running.
- There are firewalls or network routing configuration that is stopping the network connection from being established. Check firewalls on the PaperCut server or with your network administrator.
- There is a network outage that is stopping the connection being established. Try accessing the web interface on the Xerox to check that a network connection can be established.
- The PaperCut server name or IP was not set correctly.

I see an "Unexpected error communicating with server: Unknown locale input" error on the screen. How can I make this go away?

The device's display language is not English, and/or the country/region is set to a non-English-speaking country. To resolve this, configure your PaperCut application by setting the "Locale Override" to the 2-letter or 4-letter language code for the required language. See setting the locale override (optional) step in Installation.

I see an error on the Xerox LCD screen?
This may indicate a configuration issue, or maybe a software bug. Re-check your settings and restart the MFD (i.e. power-off and power-on the copier). If problems continue, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.

I have thousands of accounts representing my clients. Will the system handle this?
Yes. We have designed the system to handle thousands of Shared Accounts. Users with many accounts will also be presented with some "power options" to help them find accounts including keywords-based search.

I see an error: "Device Setup: Duplicate Device name, please see device web interface" after the device has already been successfully created.
Check if the scanner is broken, or scanning has been disabled since the device has been successfully created. If this is the case, rename the device's name in the device's

configuration page as *CurrentDeviceName%SERIALNUMBER%.* Simply append %SERIALNUMBER% placeholder in the existing device name.

For example: If your device is named **Library**, rename it to **Library%SERIALNUMBER%.**
The device will be created in PaperCut MF containing the serial number. In this example, it will show up as **Library-SN:SERIALNUMBER** where **SERIALNUMBER** is the actual device's serial number.
You can now continue to use PaperCut MF using this newly-created device. If you encounter issues, you may need to manually delete the previous device in PaperCut MF.

Alternatively, if the device was created with a broken/disabled scanner (type Xerox TouchScreen (LES) and you encountered this error because the scanner was fixed or now enabled, you need delete the previous device in PaperCut MF. The device will attempt to register and create another device.

This issue can be avoided in the future by adding the %SERIALNUMBER% placeholder when creating new devices in PaperCut MF. See steps in Install the PaperCut MF application section.

Why doesn't printing work when I print an HTML file from USB?
Starting from firmware version 22.1, we no longer support direct printing of HTML files from USB. This change simplifies the printing process and helps increase printer memory. To print an HTML file, please convert it to a supported format, such as PDF or Postscript, to ensure compatibility with the printer.

A. Appendix: Screenshots for User Information Sheets

Many organizations aim to provide detailed step-by-step instructions to their users to guide them through copier use. In addition to the screenshots in the previous sections of the manual, screenshots in this section are provided to be copied into user information sheets.