

# PaperCut MF - HP OXP Embedded Manual

---

## Contents

1	Version history.....	5
2	Overview.....	6
2.1	Consistency.....	6
2.2	Integration.....	6
2.3	Rate of development.....	6
2.4	Vendor Neutral.....	6
2.5	Security.....	6
3	Installation.....	7
3.1	Supported devices.....	7
3.2	System, access, and device requirements.....	7
3.3	Setup procedures on the device web interface.....	7
3.3.1	Log in to the device web interface.....	7
3.3.2	Determine the HP platform.....	9
3.3.3	Uninstall <i>PaperCut MF - HP FutureSmart Legacy</i> .....	9
3.3.4	Disable "Hold Off Print Job".....	11
3.4	Setup procedures on the PaperCut MF Admin web interface.....	11
3.4.1	Install PaperCut MF.....	11
4	Post-install testing.....	14
4.1	Test preparation: create test users.....	14
4.2	Simple printing and copying.....	15
4.2.1	Test preparation: configure simple test user.....	15
4.2.2	Simple printing.....	16
4.2.3	Simple copying.....	20
4.3	Advanced copying.....	23
5	Configuration.....	29
5.1	Inbound connections.....	29
5.1.1	Inbound connections to PaperCut MF Application Server.....	29
5.1.2	Inbound connections to PaperCut MF Site Servers.....	29
5.2	Security settings.....	29

5.2.1	HTTPS Security (recommended).....	29
5.2.2	Additional network security (optional) .....	31
5.3	Authentication methods.....	31
5.4	"Swipe card" authentication method.....	34
5.4.1	Supported card readers.....	35
5.4.2	HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader .....	35
5.4.3	Methods of handling card identifiers .....	38
5.5	Device functions .....	40
5.5.1	Device functions controlled and tracked by PaperCut MF.....	40
5.5.2	Device functions not controlled and tracked by PaperCut MF .....	41
5.5.3	Administrative device functions .....	43
5.6	Held print jobs settings at the device.....	45
5.6.1	Held print jobs settings that can be changed at the device .....	45
5.6.2	Held print jobs settings that can be viewed at the device .....	47
5.7	Scanning .....	47
5.7.1	PaperCut MF's Integrated Scanning .....	47
5.7.2	Device's "Scan to Email" .....	47
5.7.3	Device's "Scan to Network Folder".....	48
5.8	Job charging.....	55
5.8.1	Job Limits and Zero Stop.....	55
5.8.2	Account confirmation.....	55
5.8.3	Account selection .....	56
5.9	Language and Keyboard Layouts.....	59
5.10	Device's first screen's message .....	60
5.11	Screen headers .....	61
5.11.1	Header colors.....	61
5.11.2	Header logo .....	61
5.12	Timeouts.....	62
5.13	Config Editor .....	63
6	Known Limitations .....	74
6.1	Zero Stop for USB printing is unavailable.....	74
6.2	The application of Zero Stop during copying or faxing is delayed .....	74
6.3	The application of Zero Stop during simplex scanning is delayed .....	75
6.4	The configured user home directory network path is not auto-populated on the device's Scan to Network Folder.....	75

6.5	Some paper sizes are unsupported .....	75
6.6	Scanning continues even if the feeder or glass is empty .....	77
6.7	The "Cancel" and "Logout" buttons behave inconsistently on the PaperCut MF Integrated Scanning screens .....	77
6.8	Impact of environmental factors on Integrated Scanning .....	78
6.9	Attributes of scan job logs are unavailable .....	79
7	Uninstall <i>PaperCut MF - HP OXP</i> .....	79
7.1	Temporarily disable <i>PaperCut MF - HP OXP</i> .....	79
7.2	Permanently uninstall <i>PaperCut MF - HP OXP</i> .....	81
8	FAQ & Troubleshooting .....	82
8.1	IP addresses of the PaperCut MF Application Server .....	82
8.2	Device Status "Started (with errors)" .....	82
8.3	Swipe card authentication anomalies .....	83
8.4	"Device is not available to use" error .....	83
8.5	Device Status "Started (with errors) – Certificate error" .....	84
8.6	Administrative device functions are unavailable to users .....	84
8.7	Third-party applications are unable to use card readers .....	85
9	Appendix A: Device screens .....	86





# 1 Version history

PaperCut MF version	Date	Details
18.2.6	3 October 2018	5.2 Security settings
18.2.4	4 September 2018	5.4 "Swipe card" authentication method; 5.13 Config Editor
18.2.3	14 August 2018	5.5 Device functions; 5.13 Config Editors; 8 FAQ & Troubleshooting
18.2.0	5 July 2018	2 Overview; 3 Installation; 4 Post-install testing; 5 Configuration; 6 Known Limitations; 7 Uninstall <i>PaperCut MF - HP OXP</i> ; 8 FAQ & Troubleshooting; 9 Appendix A: Device screens
18.1.1	26 April 2018	3.1 Supported devices; 3.2 System, access, and device requirements; 5.2.1 HTTPS Security
18.1.0	3 April 2018	5.5.2 User device functions not controlled and tracked by PaperCut MF, 5.6.3 Account selection, 5.10 Config Editor, Appendix A: Supported card readers, Appendix B: Device screens
18.0.4	28 February 2018	Appendix A: Supported card readers
18.0.2	13 February 2018	New guide

## 2 Overview

This manual covers PaperCut's embedded software solution, *PaperCut MF - HP OXP*, for compatible HP FutureSmart 4 devices. For general PaperCut MF documentation, see the [PaperCut MF manual](#).

Some of the features of *PaperCut MF - HP OXP* include:

- Secure access to the device via user authentication
- Print release of held print jobs (Secure & Find Me Printing)
- Monitoring, control and tracking of printing, copying, scanning, and faxing (Quotas, Charging, Allocation, Job Limiting, Zero Stop, and Logging)
- Integrated Scanning
- Card self-association and print release at login
- Allocation of printing, copying, scanning, and faxing costs to different accounts, departments, cost centers, or projects (Shared Accounts)
- Multiple ways to locate Shared Accounts
- Adding comments to invoices of Shared Accounts
- Customization of most device screens, including logos, colors, and messages
- Changing and viewing the settings of held print jobs at the device

Highlights of PaperCut's embedded software solution include:

### 2.1 Consistency

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

### 2.2 Integration

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

### 2.3 Rate of development

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

### 2.4 Vendor Neutral

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

### 2.5 Security

All embedded solutions are developed with both network and application security in mind, offering features like Secure & Find Me Printing, as well as use of SSL network protocols.

## 3 Installation

This section covers the installation of *PaperCut MF - HP OXP*.

### 3.1 Supported devices

Ensure that the devices on the network are HP FutureSmart 4 devices that are listed as supported devices on the [PaperCut MF for HP](#) page.

### 3.2 System, access, and device requirements

Ensure that the following system, access, and device requirements are met:

- The following entities are available:
  - Physical device – administrator and user access, and credentials
  - Device's web interface – administrator access, URL, and credentials
  - PaperCut MF Admin web interface – administrator access, URL, and credentials
- The supported HP FutureSmart 4 devices on the network are compatible with PaperCut's embedded software solution, *PaperCut MF - HP OXP*. For more information, see [3.3.1 Log in to the device web interface](#) and [3.3.2 Determine the HP platform](#).
- The latest version of PaperCut MF is installed and running on the network. For more information, see the [PaperCut MF manual](#).
- **Note:** The minimum compatible version is 18.0.2.
- The devices on the network are directly accessible by the PaperCut MF Application Server (i.e. not via a NAT network).
- The networking/firewall configuration allows:
  - Inbound connections to the PaperCut MF Application Server from the devices on the configured ports. For example:
    - 9191 (TCP/HTTP)
    - 9192 (SSL/TLS/HTTPS)
  - Outbound connections from the PaperCut MF Application Server to the devices on the configured ports. For example:
    - 80 (TCP/HTTP)
    - 443 (SSL/TLS/HTTPS)

### 3.3 Setup procedures on the device web interface

#### 3.3.1 Log in to the device web interface

To access the device's web interface as an administrator:

1. Log in to the device's web interface.
2. In **Local Device Account**, select **Administrator**:

**Sign In**

Sign In Method  
Local Device

**Local Device Account**  
Administrator

Password

3. If this device's web interface is being accessed for the first time:
  - a. Do not enter a password
  - b. Click **Sign in**.
  - c. Navigate to **Security > General Security**.
  - d. Set the administrator credentials:

Information General Copy/Print Scan/Digital Send Fax Troubleshooting **Security** HP Web Services Netw

**General Security**

Account Policy  
Access Control  
Protect Stored Data  
Certificate Management  
Web Service Security  
Self Test

**Set the Local Administrator Password**

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

User Name  
admin

Old Password New Password Verify Password

- e. Click **Apply**.
4. If this device's web interface has been accessed previously:
  - a. Enter the administrator password.
  - b. Click **Sign in**:

**Sign In**

Sign In Method  
Local Device

Local Device Account  
Administrator

**Password**

**Sign In** Cancel

HP Instant Support | Shop for Supplies | Product Support  
© Copyright 2010-2017 HP Development Company, L.P.

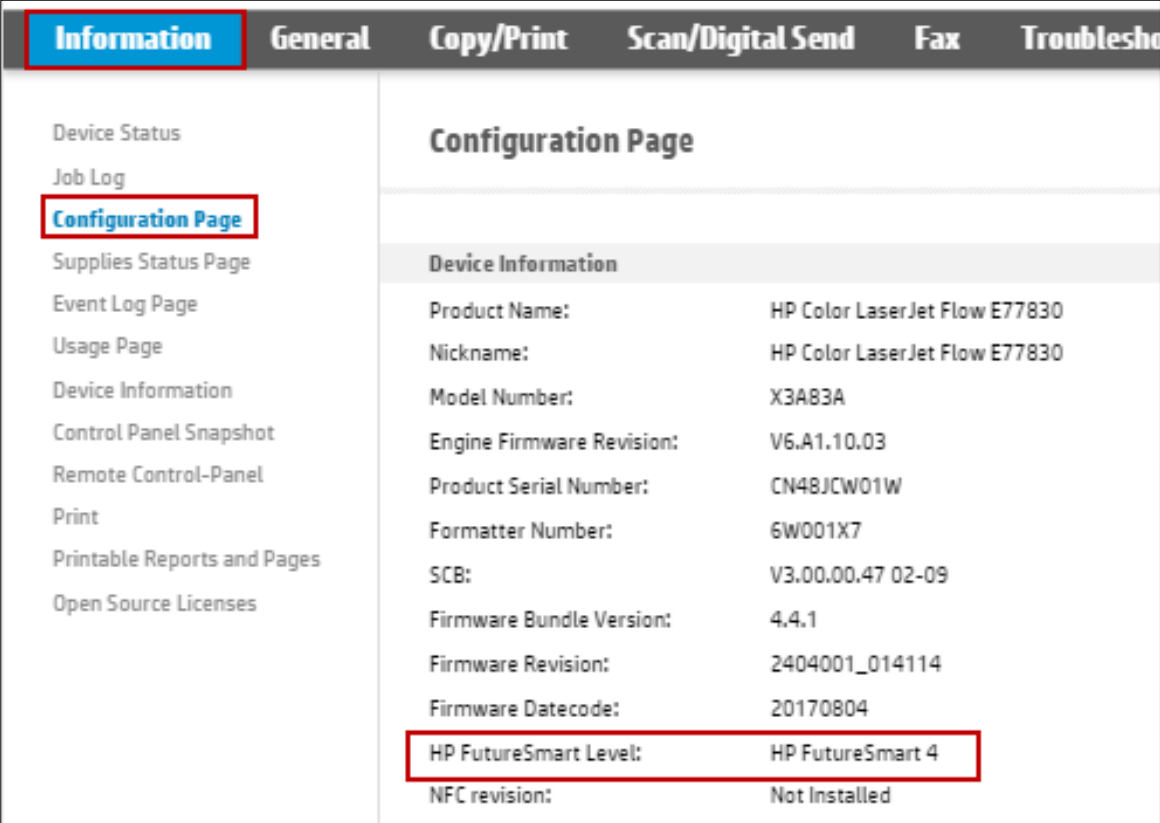


### 3.3.2 Determine the HP platform

Before attempting to install *PaperCut MF - HP OXP*, you must ensure that it is running the HP FutureSmart 4 platform.

To determine the HP platform:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Information > Configuration Page**.
3. Verify that the **Device Information** area's field **HP FutureSmart Level** displays **HP FutureSmart 4**:



Configuration Page	
<b>Device Information</b>	
Product Name:	HP Color LaserJet Flow E77830
Nickname:	HP Color LaserJet Flow E77830
Model Number:	X3A83A
Engine Firmware Revision:	V6.A1.10.03
Product Serial Number:	CN48JCW01W
Formatter Number:	6W001X7
SCB:	V3.00.00.47 02-09
Firmware Bundle Version:	4.4.1
Firmware Revision:	2404001_014114
Firmware Datecode:	20170804
<b>HP FutureSmart Level:</b>	<b>HP FutureSmart 4</b>
NFC revision:	Not Installed

**Note:** This manual is relevant only if the device is running the **HP FutureSmart 4** platform (i.e. HP FutureSmart 4 devices). For more information on PaperCut's embedded software solutions for other devices and platforms, contact your reseller or Authorized Solution Center.

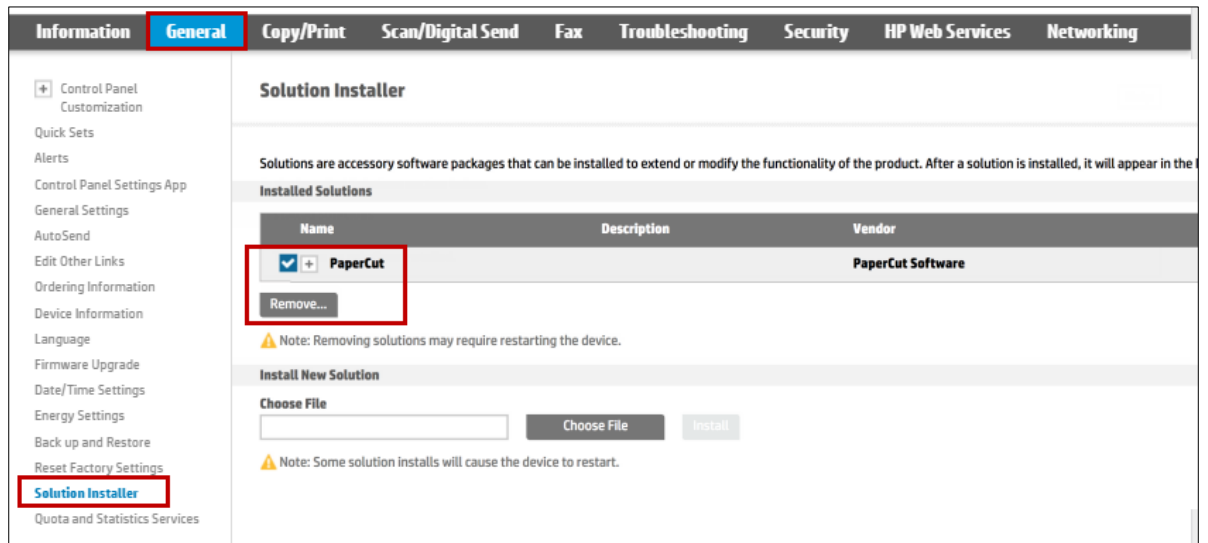
### 3.3.3 Uninstall *PaperCut MF - HP FutureSmart Legacy*

Before attempting to install *PaperCut MF - HP OXP*, ensure that PaperCut's embedded software solution *PaperCut MF - HP FutureSmart Legacy*, is not already installed. If it is already installed, the you must first uninstall the existing *PaperCut MF - HP FutureSmart Legacy* before attempting to install *PaperCut MF - HP OXP*.

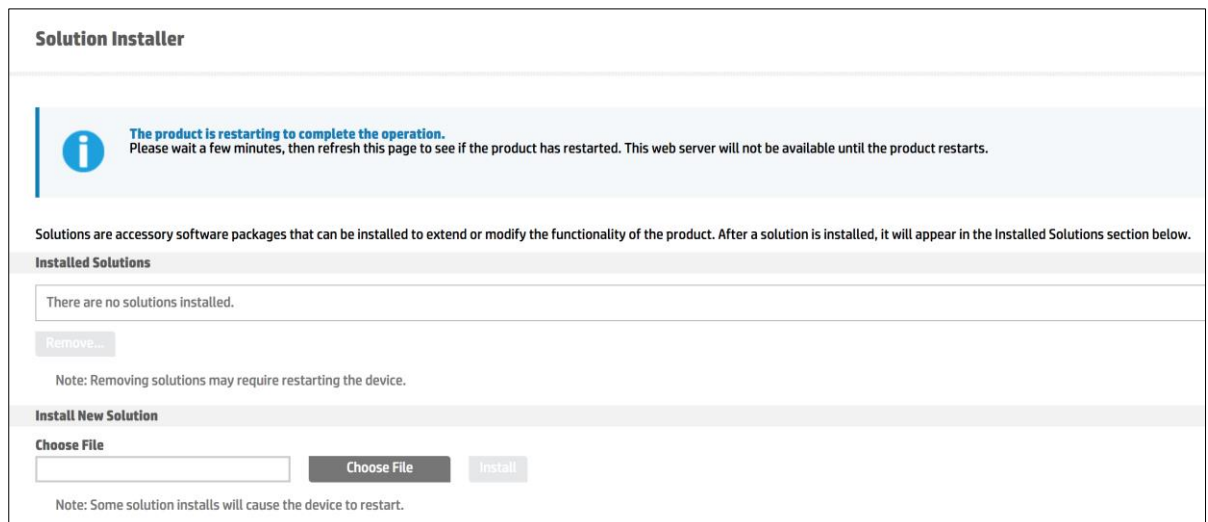
To uninstall *PaperCut MF - HP FutureSmart Legacy*:

1. Log in to the device's web interface as an administrator.
2. Navigate to **General > Solution Installer**.
3. Select **PaperCut**.

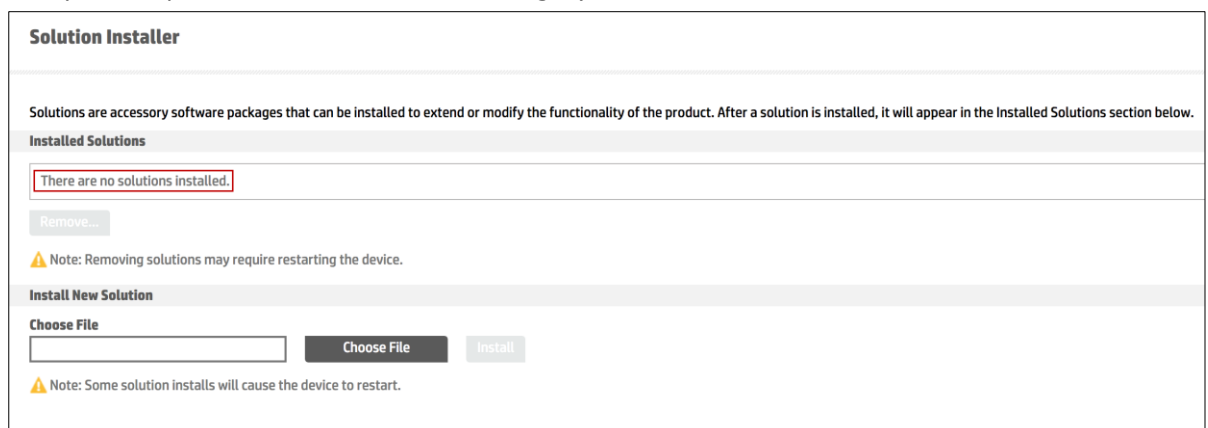
4. Click **Remove...**



The device reboots and restarts to uninstall *PaperCut MF - HP FutureSmart Legacy* from the device:



5. Verify that *PaperCut MF - HP FutureSmart Legacy* is uninstalled from the device:

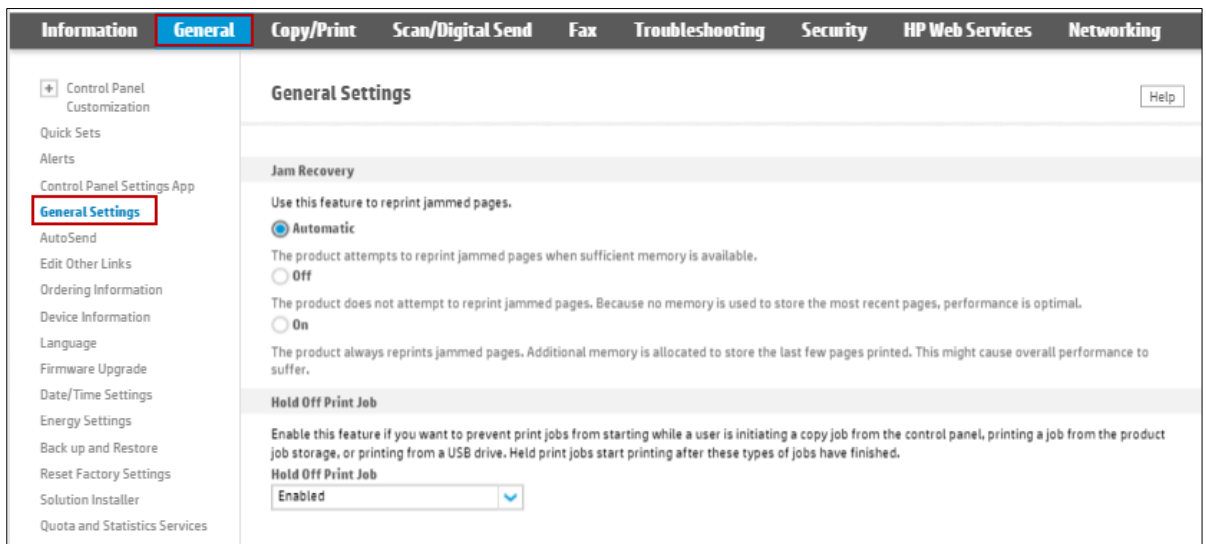


### 3.3.4 Disable "Hold Off Print Job"

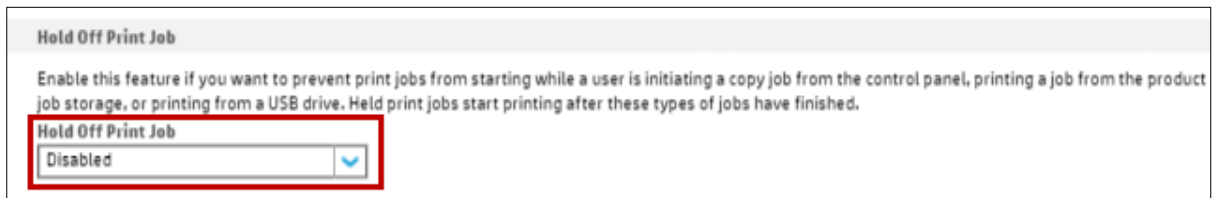
Before attempting to install *PaperCut MF - HP OXP* on the device, you must disable the device's "Hold Off Print Job" setting. This setting is enabled by default, delaying printing by 15 seconds from when the user releases the held print job.

To disable "Hold Off Print Job":

1. Log in to the device's web interface as an administrator.
2. Navigate to **General > General Settings**:



3. Change the **Hold Off Print Job** setting from **Enabled** to **Disabled**.



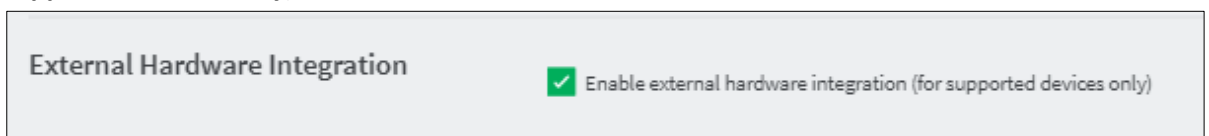
4. Click **Apply**.

## 3.4 Setup procedures on the PaperCut MF Admin web interface

### 3.4.1 Install PaperCut MF

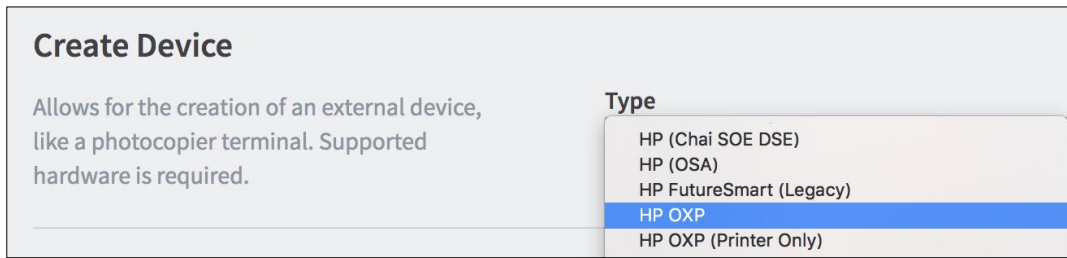
To install PaperCut MF (i.e. device registration and integration):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **External Hardware Integration** area, select **Enable external hardware integration (for supported devices only)**.



4. Click **Apply**.
5. Navigate to **Devices**.
6. Click **Create Device**.

- In **Type**, select **HP OXP**:



- In **Device name**, enter a descriptive name for the device.
- Optionally, in **Location/Department**, enter location or department details of the device.
- In **Hostname / IP**, enter the network name or IP address of the device.
- In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device's web interface. For more information, see [3.3.1 Log in to the device web interface](#).
- In **Function**, select the relevant device functions:

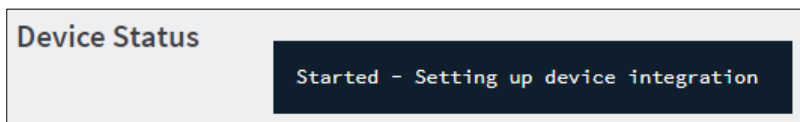
- **Track & control copying**
- **Track & control scanning**
- **Track & control faxing**
- **Enable print release**

**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. For more information on configuring the printer queue's Hold/Release Queue Settings, see the [PaperCut MF manual](#).

**Note:** For more information, see [5.5 Device functions](#).

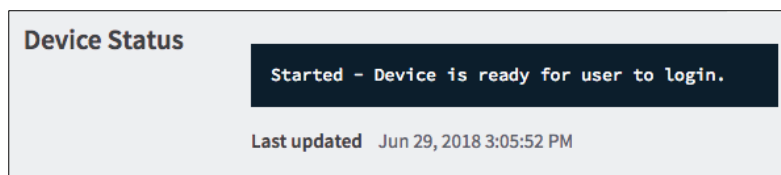
- Click **Ok**.

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



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

- The **Device Status** displays the status **Started - Device is ready for user to login**:

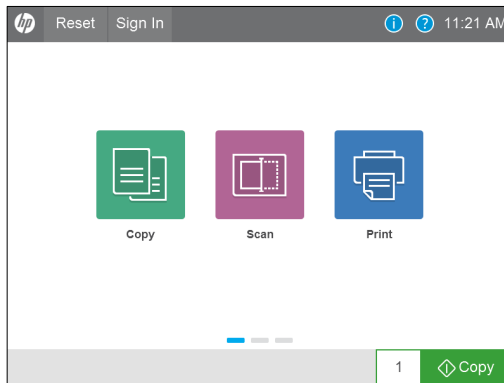


**Note:** If the Device Status displays any other status, then see [8.2 Device Status "Started \(with errors\)"](#).

- Based on the device's **HP FutureSmart 4 Firmware Bundle Version**, the device's first screen and the resulting workflow actions could be any one of the following:

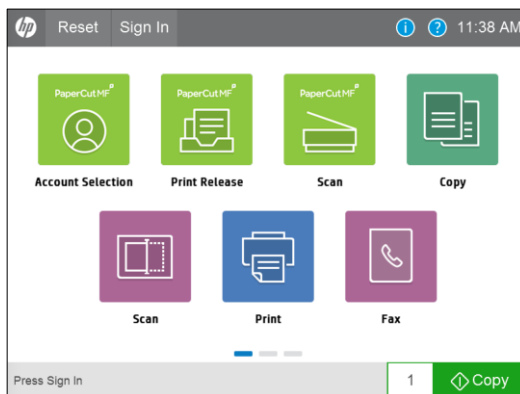
<b>HP FutureSmart 4 Firmware Bundle Version 4.5.2</b>	<b>HP FutureSmart 4 Firmware Bundle Version 4.5.5</b>
---	---

The first screen on the device is a non-PaperCut MF screen with the following icons:



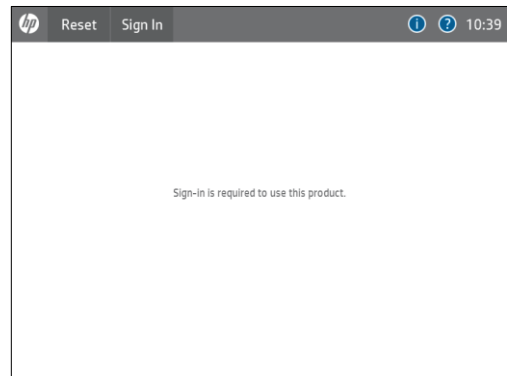
Click **Reset**.

Verify that the first non-PaperCut MF device screen now displays PaperCut MF icons:



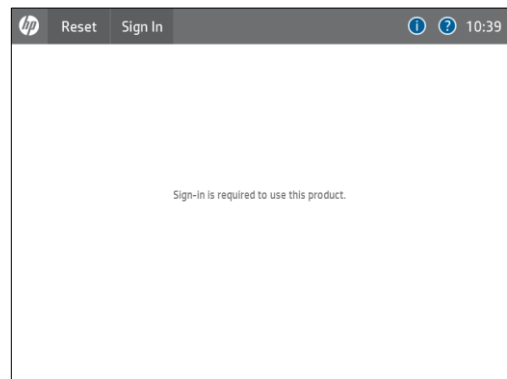
Users may access the PaperCut MF Login screen by clicking **Sign In**, any other application on the device, or by using their swipe cards (if the **Swipe card** authentication method is selected).

The first screen on the device is a non-PaperCut MF screen with the following default message:



Click **Reset**.

Verify that the first non-PaperCut MF device screen continues to display the same default message:



Users may access the PaperCut MF Login screen by based on the above default message, which can be customized (either by clicking **Sign In** or by using their swipe cards, if the **Swipe card** authentication method is selected).

**Note:** You may also customize this default message. For more information, see [5.10 Device's first screen's message](#).

**Note:** If the following warning is displayed on the PaperCut MF Admin web interface, then see [5.2.1 HTTPS Security \(recommended\)](#):

⚠
Enable SSL to secure communication between PaperCut and the device. Refer to embedded manual to enable SSL.

## 4 Post-install testing

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

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

This section covers the following post-install testing scenarios for *PaperCut MF - HP OXP*:

- [4.2 Simple printing and copying](#)
- [4.3 Advanced copying](#)

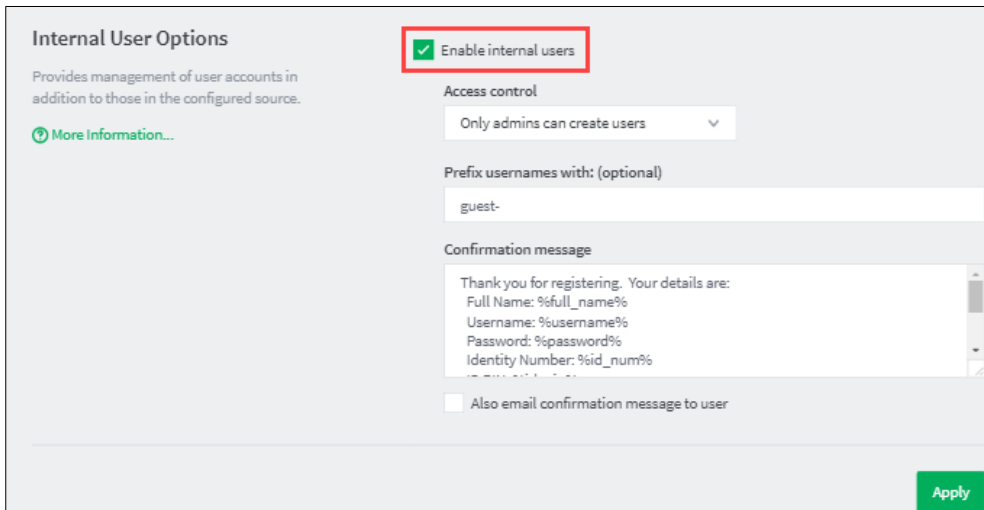
### 4.1 Test preparation: create test users

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

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

To create test users:

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



**Internal User Options**  
Provides management of user accounts in addition to those in the configured source.  
[More Information...](#)

Enable internal users

Access control  
Only admins can create users

Prefix usernames with: (optional)  
guest-

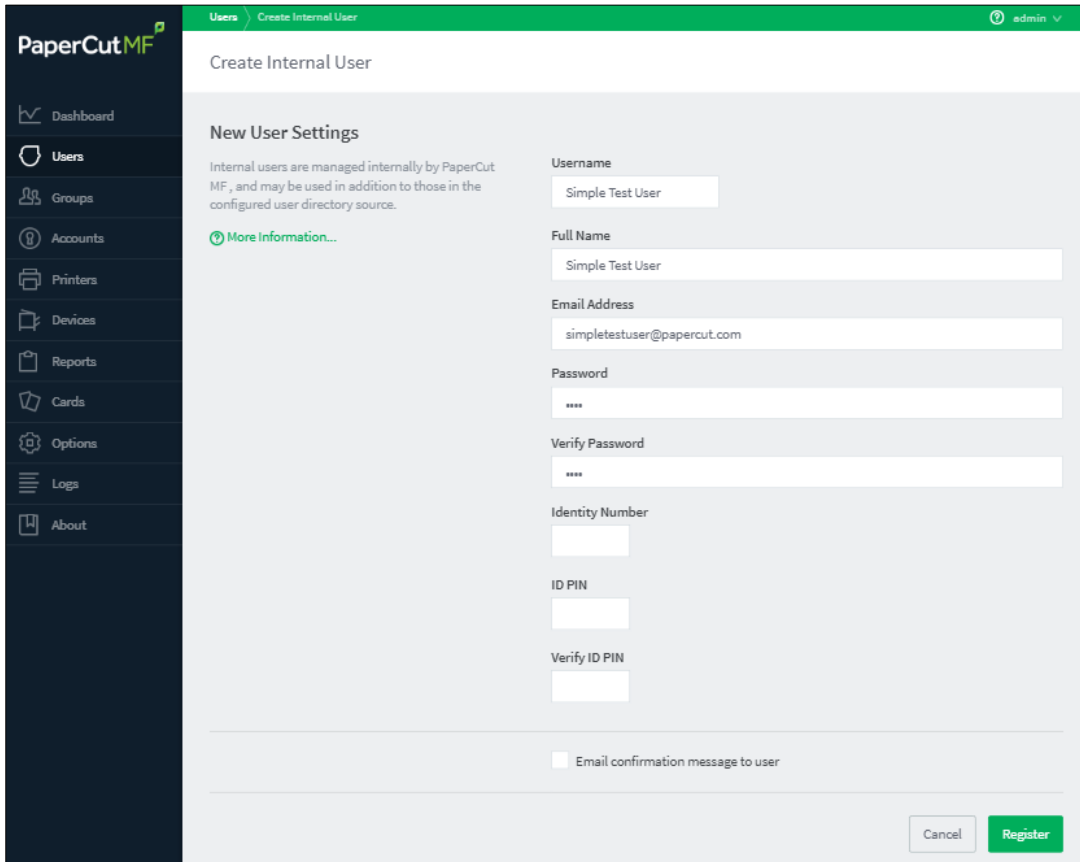
Confirmation message  
Thank you for registering. Your details are:  
Full Name: %full\_name%  
Username: %username%  
Password: %password%  
Identity Number: %sid\_num%

Also email confirmation message to user

Apply

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

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



The screenshot shows the 'Create Internal User' form in the PaperCut MF Admin interface. The form is titled 'New User Settings' and includes the following fields:

- Username: Simple Test User
- Full Name: Simple Test User
- Email Address: simpletestuser@papercut.com
- Password: \*\*\*\*
- Verify Password: \*\*\*\*
- Identity Number: [Empty field]
- ID PIN: [Empty field]
- Verify ID PIN: [Empty field]

There is also a checkbox for 'Email confirmation message to user' which is currently unchecked. At the bottom right, there are 'Cancel' and 'Register' buttons.

8. Click **Register**.

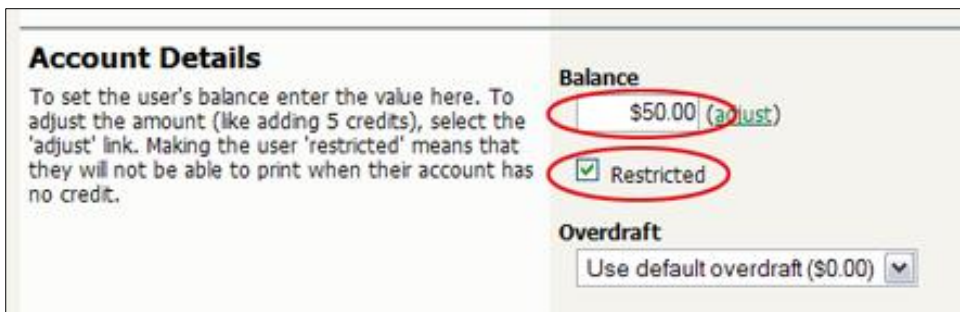
## 4.2 Simple printing and copying

### 4.2.1 Test preparation: configure simple test user

To test the simple test scenarios, ensure at least one simple test user is created. For more information, see [4.1 Test preparation: create test users](#). Once created, ensure the simple test user is configured.

To configure the simple test user:

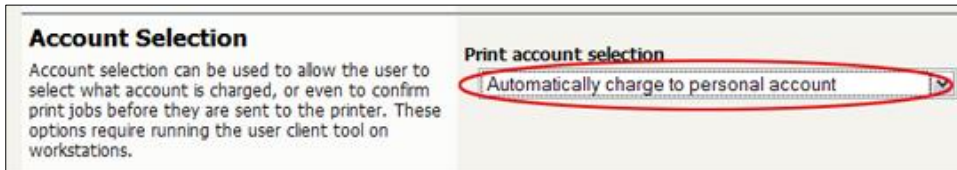
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Users**.
3. From the **User List**, select the simple test user.
4. In the **Account Details** area, set the **Balance** to **\$50.00** and select **Restricted**:



The screenshot shows the 'Account Details' form for a user. The form includes the following fields:

- Balance**: \$50.00 (adjust)
- Restricted**:
- Overdraft**: Use default overdraft (\$0.00)

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



6. Click **Apply**.

## 4.2.2 Simple printing

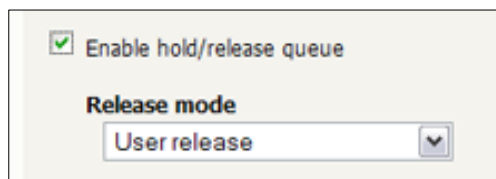
Simple printing does not involve providing the simple test user with a choice of accounts to choose from. Printing is charged to the simple test user's default My Personal Account.

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

- **Simple test user** - A simple test user is created and configured. For more information, see [4.1 Test preparation: create test users](#) and [4.2.1 Test preparation: configure simple test user](#).
- **Printer queue settings** - The printer queue's Hold/Release Queue Settings are configured. For more information, see the [PaperCut MF manual](#).

To configure the printer queue's Hold/Release Queue Settings:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Printers**.
3. Select the Printer that is applicable to the device being tested.
4. In the **Hold/Release Queue Settings** area, select the **Enable hold/release queue**.



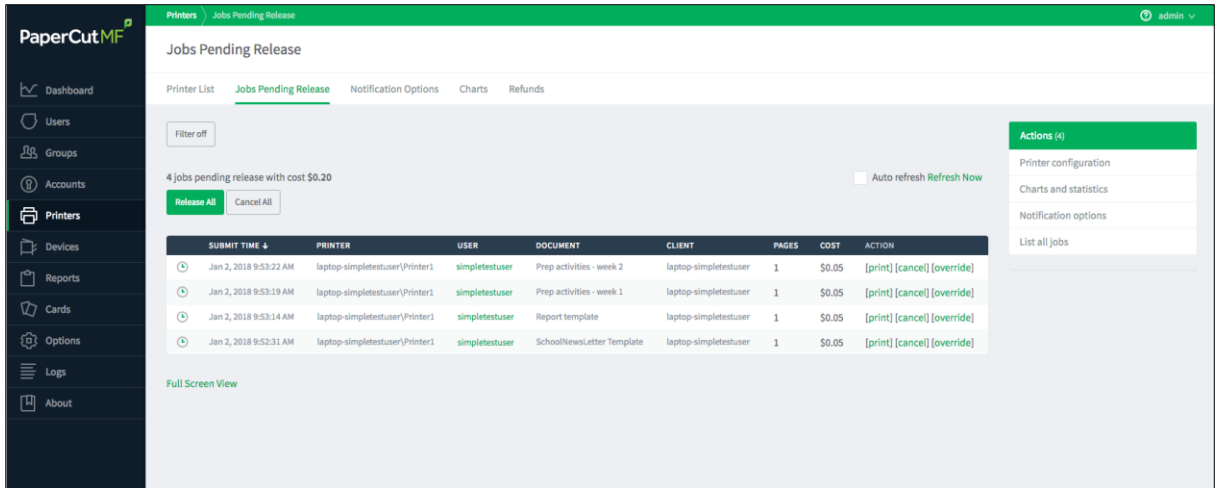
5. Click **Apply**.  
Print jobs to this printer queue are held until released by a user.
- **Device functions** – The printing function is enabled.  
To enable the printing function:
    1. Log in to the PaperCut MF Admin web interface.
    2. Navigate to **Devices**.
    3. Select the device being tested.
    4. In the **Print Release** area, select **Enable print release**.
    5. In the **This device will display jobs for release from the selected source queues**, select at least one source queue for print release that corresponds to this device's configured printer queue.
    6. Click **Apply**.
    7. Verify that the **Devices > External Device List** displays the device with **Print Release** in the **Function** column.

To test simple printing:

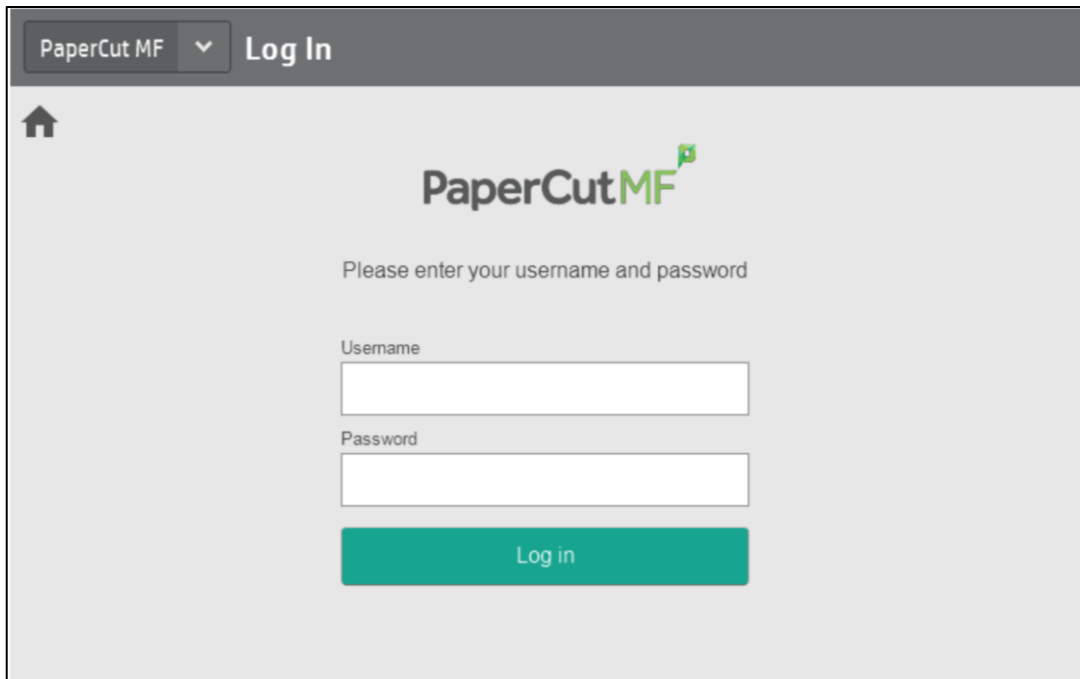
1. Log in to a computer as the simple test user.



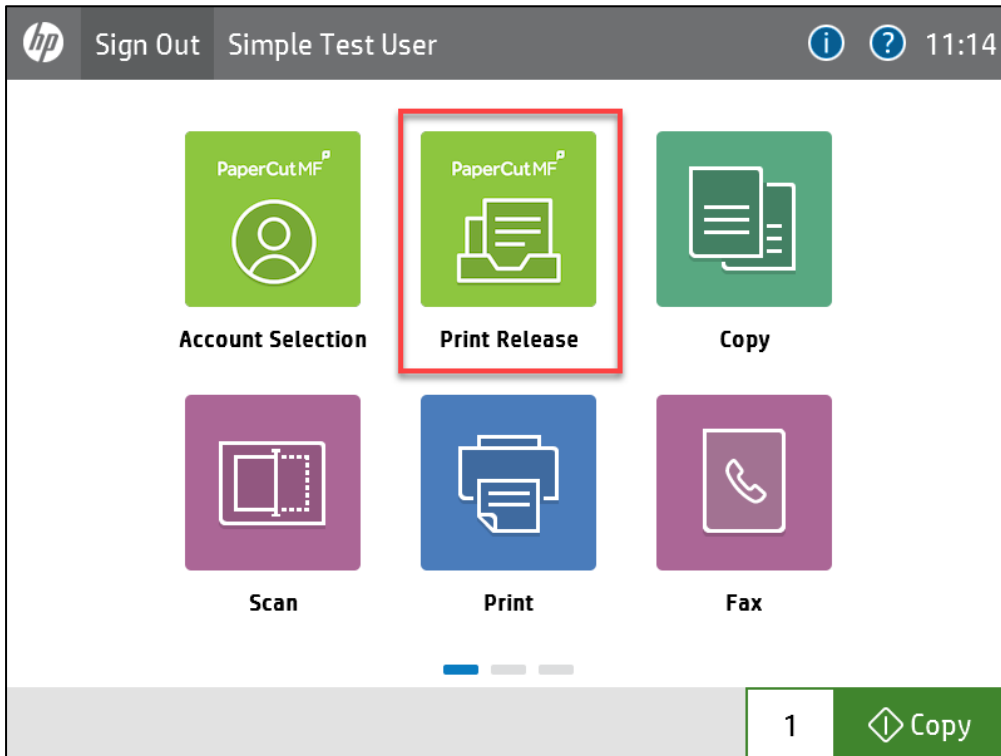
2. Print a few jobs to the source queue that was selected in the **Devices > External Device List > Device Details > Print Release > Enable print release** area of the device being tested.
3. Log in to the PaperCut MF Admin web interface.
4. Navigate to **Printers > Jobs Pending Release**.
5. Verify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



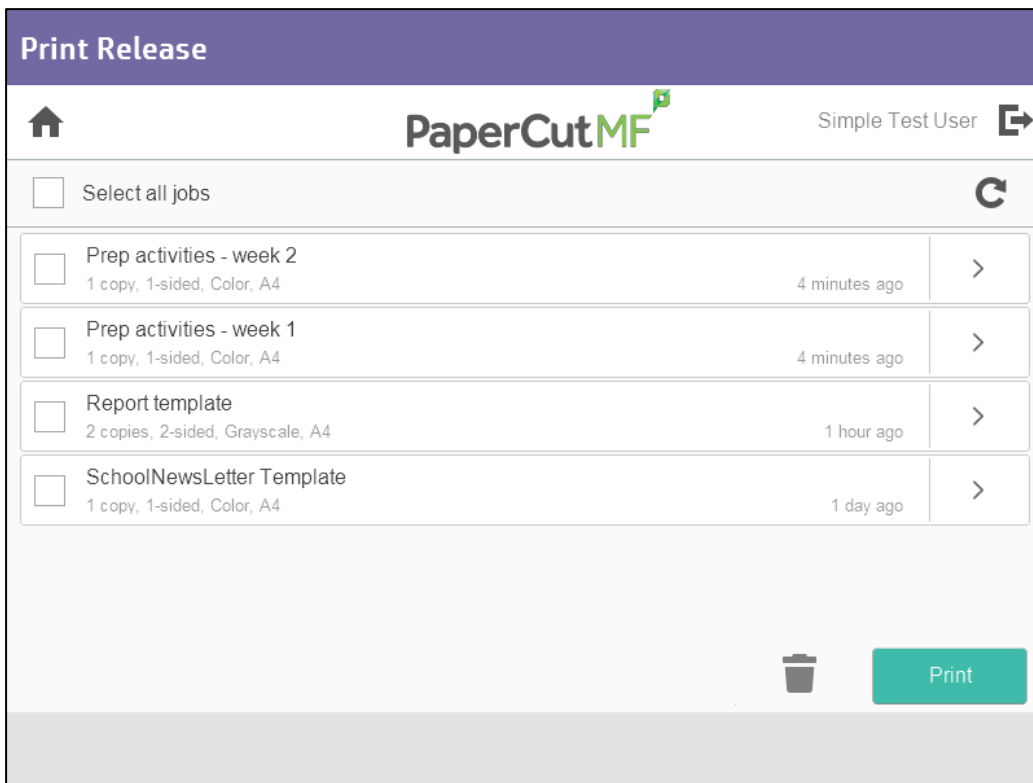
6. Log out of the PaperCut MF Admin web interface.
7. Log in to the device as the simple test user:



8. Select **Print Release**:



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



**Note:** You may be able to change the settings of held print jobs on the PaperCut MF Print Release screen before releasing them. For more information, see [5.6 Held print jobs settings at the device](#).

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

11. To delete one or many held print jobs at once, select all the relevant held print jobs and click the **Bin** icon.
12. To view and take actions on a single held print job, click the chevron:



Details of the held print job are displayed:

**Print Settings**

<
PaperCut<sup>®</sup>MF
Simple Test User ➤

Print Release > Prep activities - week 1

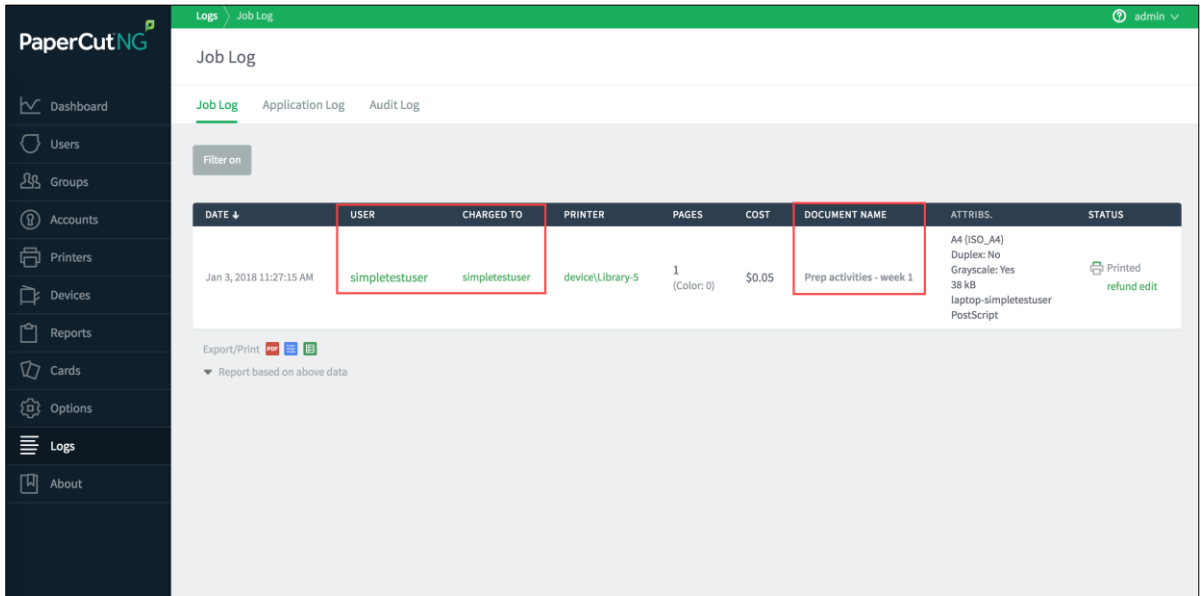
<b>Time</b>	Jun 22, 2018 10:53:57 AM	<b>Copies</b>	1
<b>User</b>	simpletestuser	<b>Duplex mode</b>	1-sided
<b>Pages</b>	3	<b>Color mode</b>	Color
<b>Account</b>	DEFAULT	<b>Page size</b>	A4
<b>Balance</b>	\$100.00	<b>Cost</b>	\$0.51

Print

**Note:** You may be able to change the settings of held print jobs on the PaperCut MF Print Settings screen before releasing them. For more information, see [5.6 Held print jobs settings at the device](#).

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

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



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

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

### 4.2.3 Simple copying

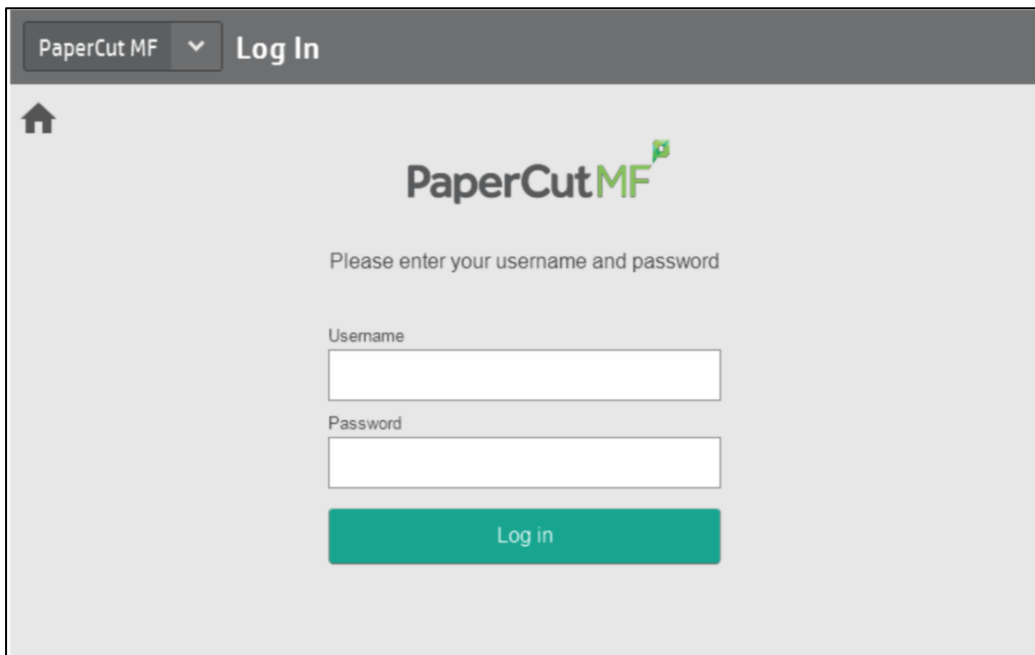
Simple copying does not involve providing the simple test user with a choice of accounts to choose from. Copying is charged to the simple test user's default My Personal Account.

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

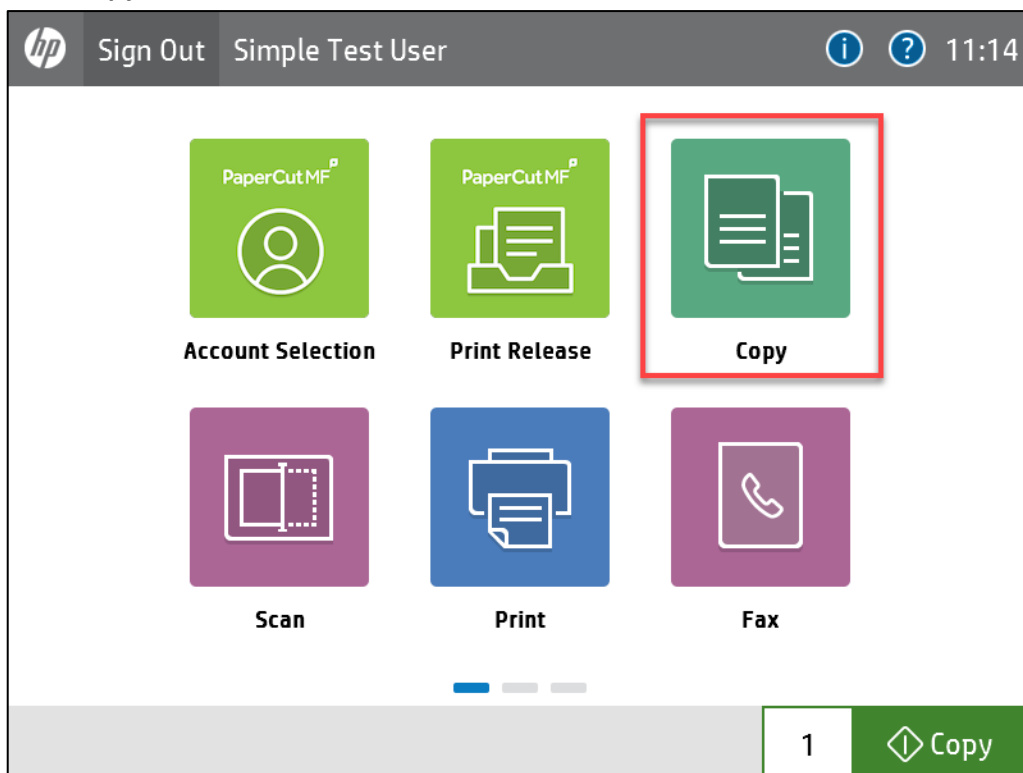
- **Simple test user** - A simple test user is created and configured. For more information, see [4.1 Test preparation: create test users](#) and [4.2.1 Test preparation: configure simple test user](#).
- **Device functions** – The copying function is enabled. To enable the copying function:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Devices**.
  3. Select the device being tested.
  4. In the **External Device Settings > Tracking** area, select **Track & control copying**.
  5. Click **Apply**.
  6. Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.

To test simple copying:

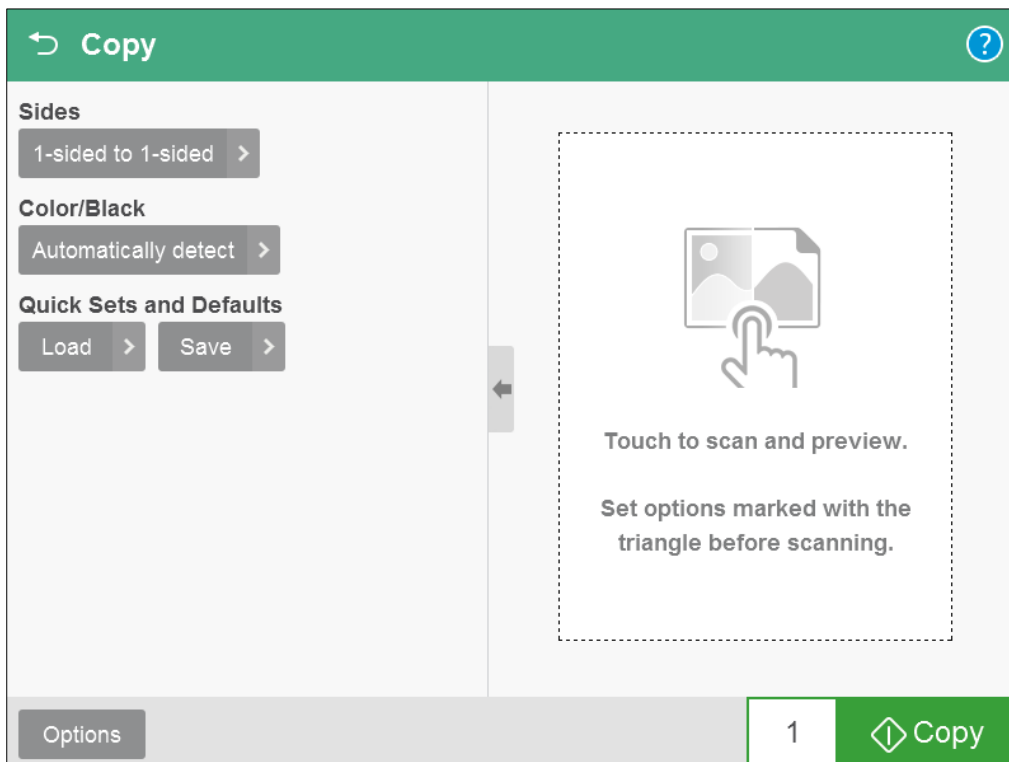
1. Log in to the device as the simple test user:



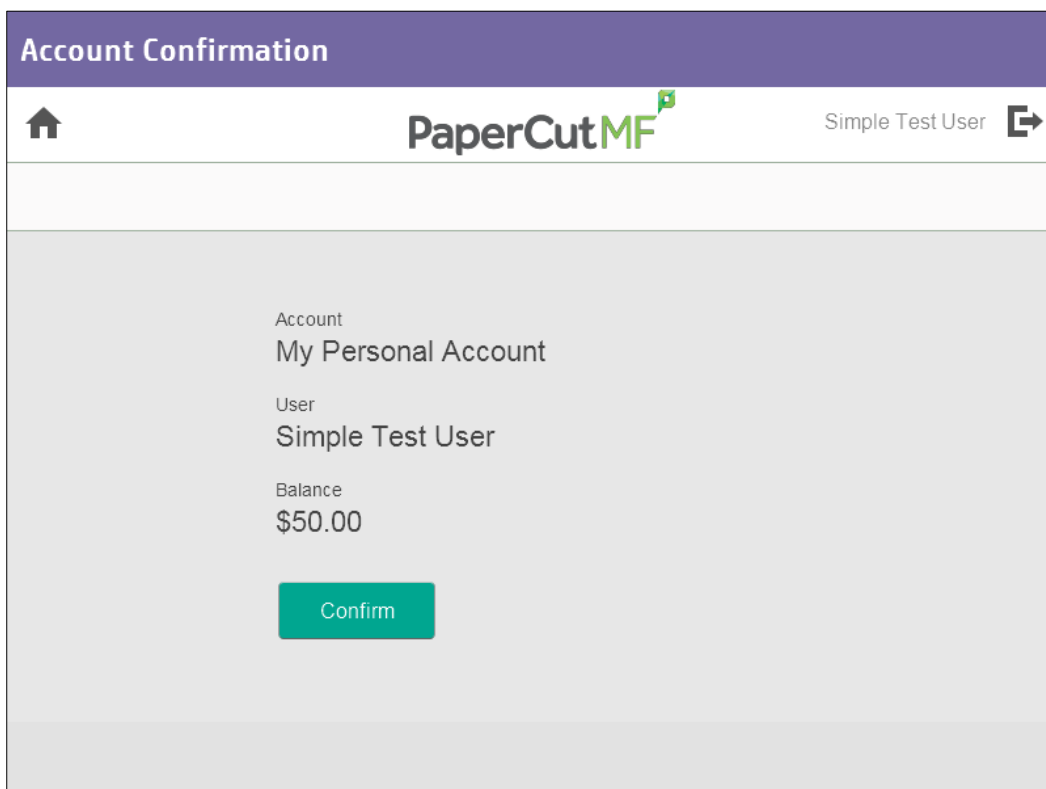
2. Select **Copy**:



3. Continue copying by following the device's workflow:

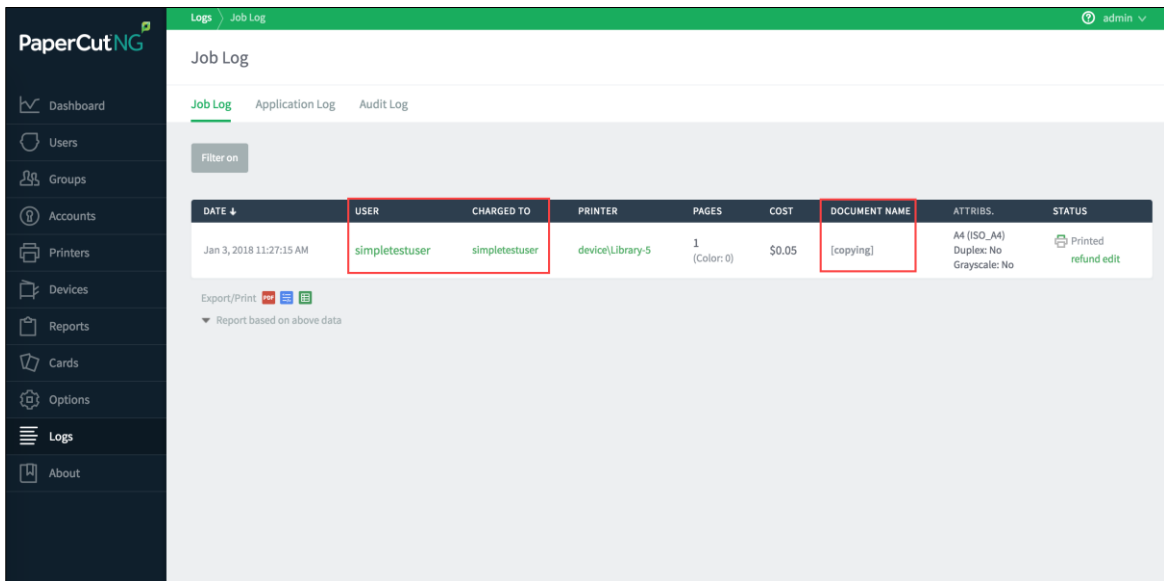


4. Verify that the PaperCut MF Account Confirmation screen does not provide the simple test user with a choice of accounts to choose from, and charges copying to the simple test user's default My Personal Account:



5. Click **Confirm**.
6. Complete copying.
7. Log out of the device.

8. Log in to the PaperCut MF Admin web interface.
9. Navigate to **Logs**.
10. After copying is completed, verify that **Job Log** page displays the test user's name, simple test user, in the **User** column and the **Charged To** column:



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

### 4.3 Advanced copying

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

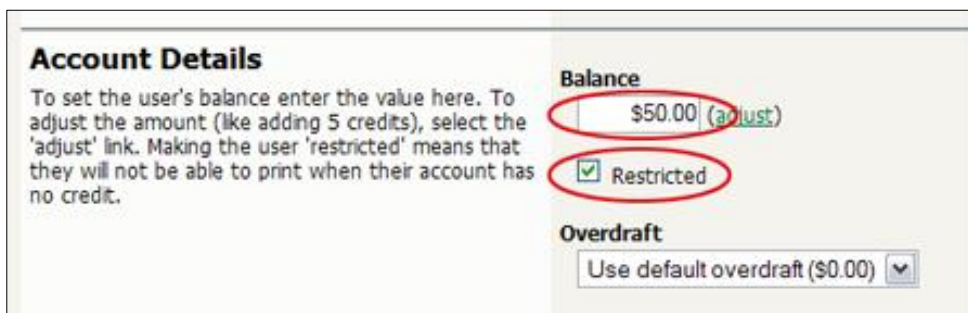
To test advanced copying, ensure the following test preparation requirements are met:

- **Advanced test user** – An advanced test user must be created. For more information, see [4.1 Test preparation: create test users](#).

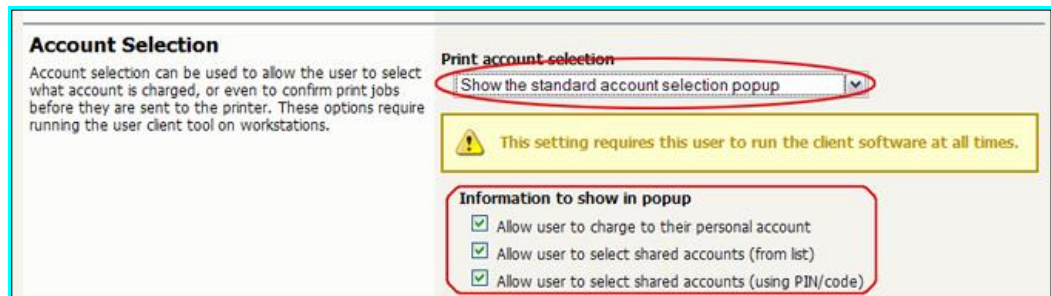
Once created, the advanced test user must be configured.

To configure the advanced test user:

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



- In the **Account Selection** area's **Print account selection**, select **Standard account selection popup** and in **Information to show in popup**, select all the options:



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

**Print account selection**  
Show the standard account selection popup

**Information to show in popup**

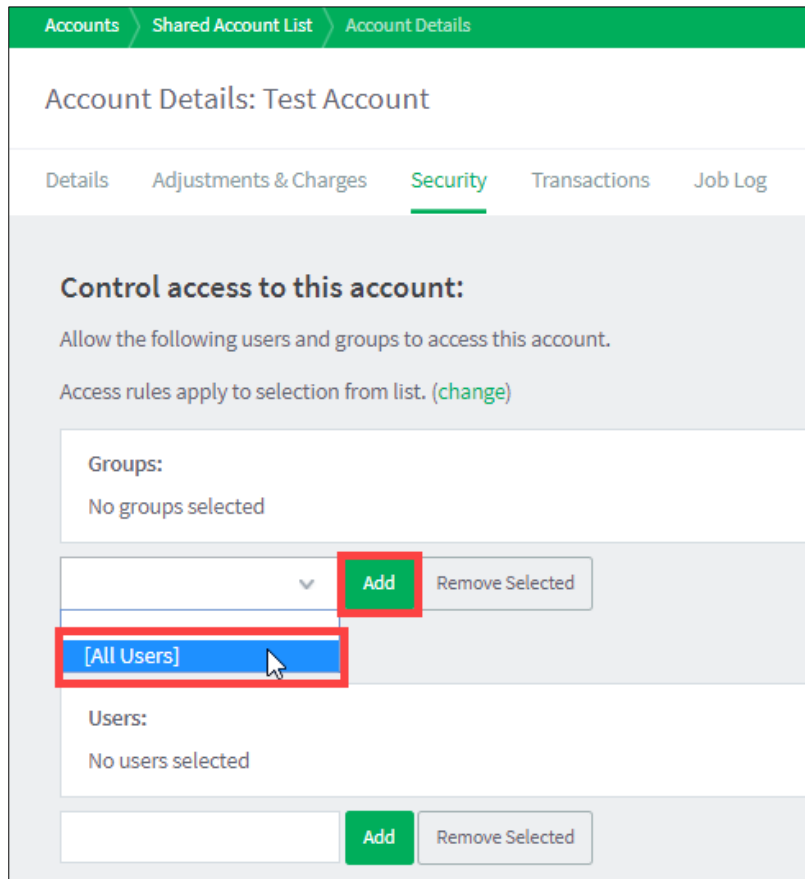
- Allow user to charge to their personal account
- Allow user to select shared accounts (from list)
- Allow user to select shared accounts (using PIN/code)

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

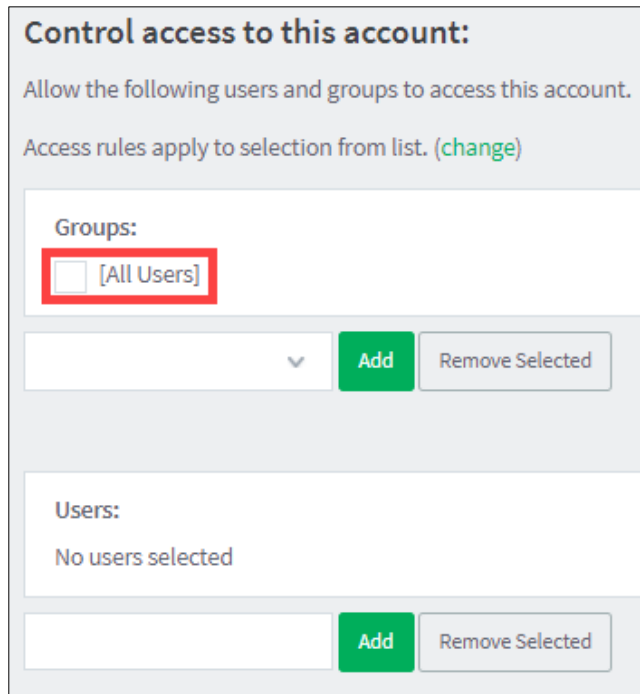
- Click **Apply**.
- Device functions** – The copying function is enabled.  
To enable the copying function:
    - Log in to the PaperCut MF Admin web interface.
    - Navigate to **Devices**.
    - Select the device being tested.
    - In the **External Device Settings > Tracking** area, select **Track & control copying**.
    - Click **Apply**.
    - Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.
  - Advanced account** – A test account is created.  
To create a test account:
    - Log in to the PaperCut MF Admin web interface.
    - Navigate to **Accounts**.
    - Click **Create a new account....**
    - In the **Details & Balance** area's field **Account Name**, enter the name of the test account (test account).
    - Click **Apply**.
    - Verify that the **Accounts > Shared Account List** page displays the test account created.
    - Click the test account.
    - Navigate to **Security**.



- In the **Control access to this account > Groups** area, select [All Users] and click Add:

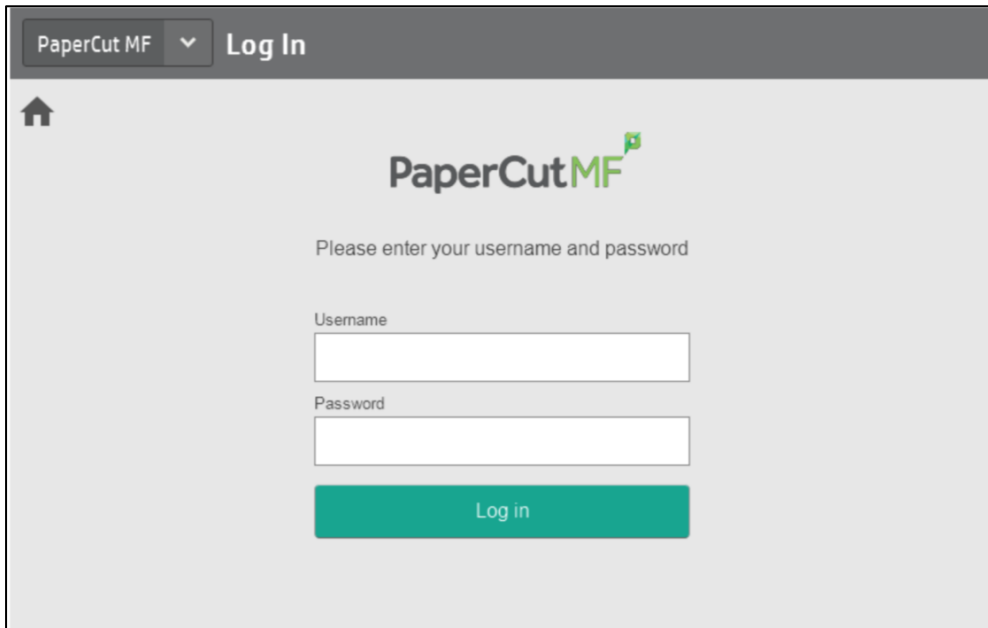


- Verify that the **Control access to this account > Groups** area displays [All Users]:

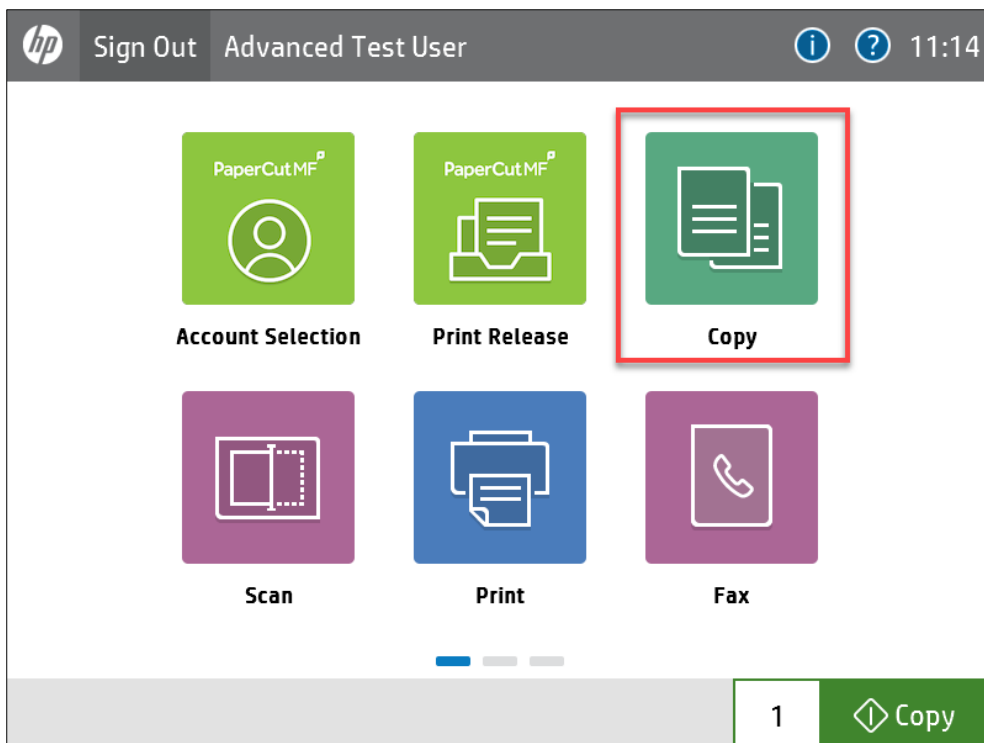


To test advanced copying:

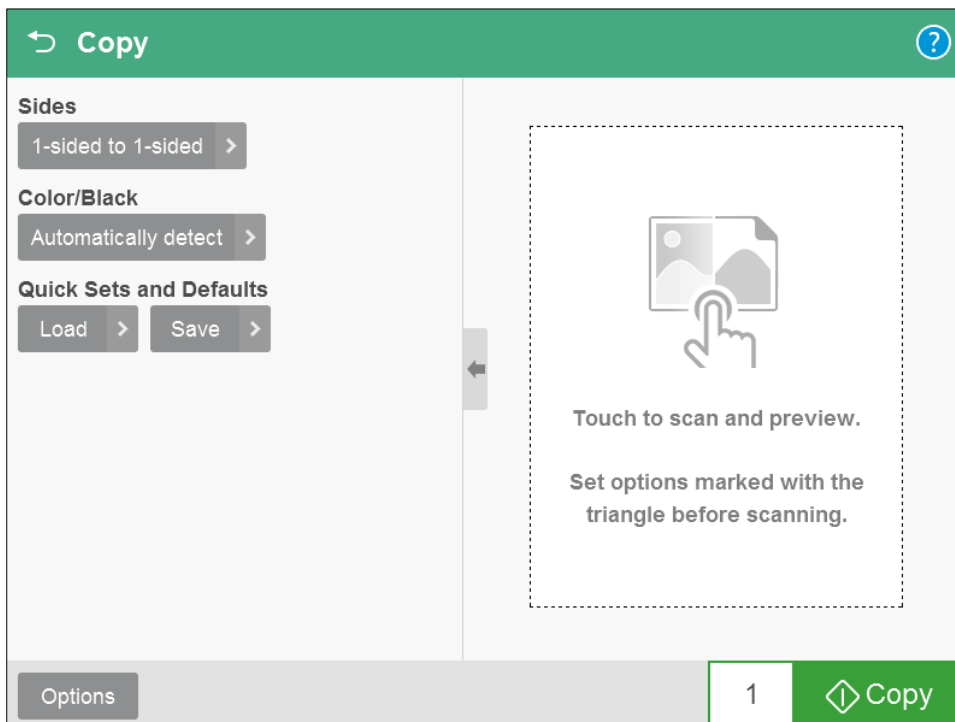
1. Log in to the device as the simple test user:



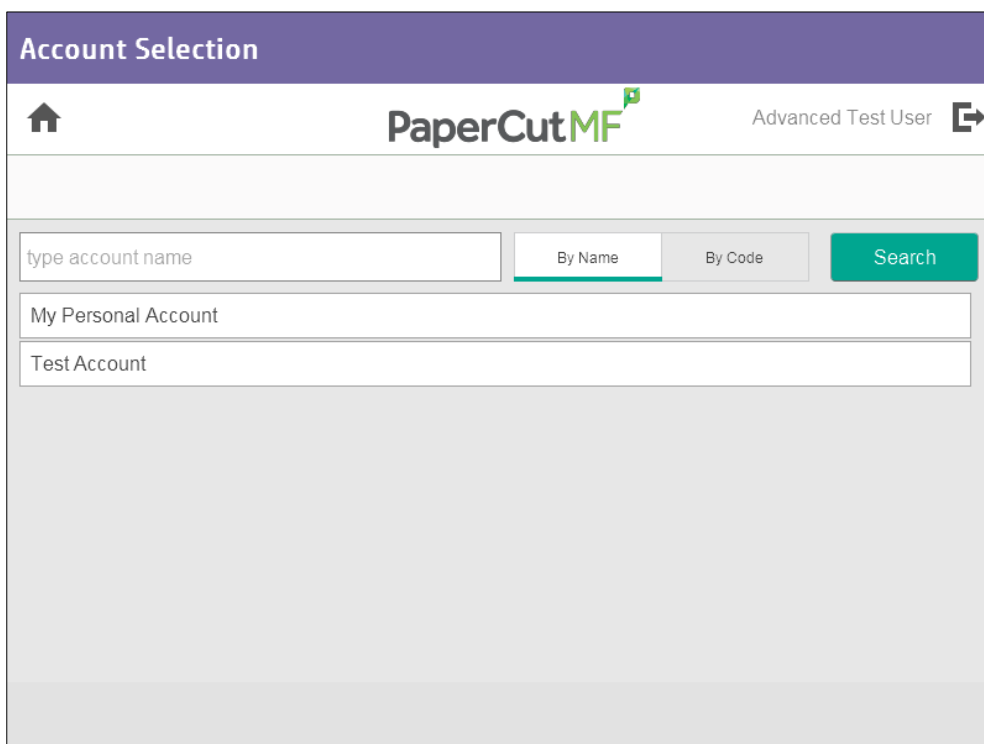
2. Select **Copy**:



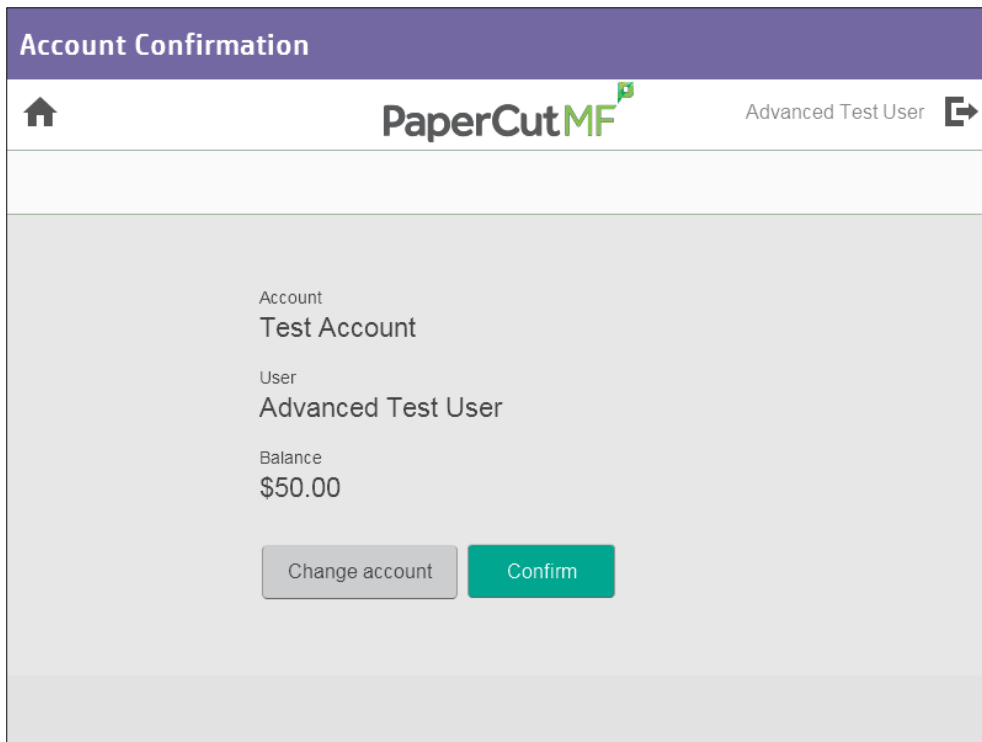
- Continue copying by following the device's workflow:



- Verify that the PaperCut MF Account Selection screen provides the advanced test user with a choice of accounts to choose from:



- Select the relevant account, test account.
- Verify that the PaperCut MF Account Confirmation screen displays the selected account, test account, but continues to provide the advanced test user with the option of changing the account:



7. Click **Confirm**.  
Copying is charged to the account selected by the advanced test user, test account.
8. Complete copying.
9. Log out of the device.
10. Log in to the PaperCut MF Admin web interface.
11. Navigate to **Logs**.
12. After copying is completed, verify that **Job Log** page displays the test user's name, advanced test user, in the **User** column and the selected account's name, test account, in the **Charged To** column:

PaperCut<sup>®</sup>NG

Logs Job Log

Job Log Application Log Audit Log

Filter on

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

Export/Print

Report based on above data

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

## 5 Configuration

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

This section covers the configuration changes that can be made to the default settings of *PaperCut MF - HP OXP*.

### 5.1 Inbound connections

#### 5.1.1 Inbound connections to PaperCut MF Application Server

To configure PaperCut MF to allow inbound connections from the device to the PaperCut MF Application Server, use the config key **system.network-address**. For more information, see [5.13 Config Editor](#).

#### 5.1.2 Inbound connections to PaperCut MF Site Servers

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

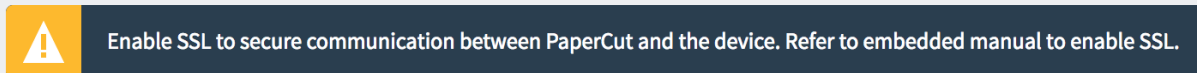
1. Site Servers must already be installed and configured. For more information, see the [PaperCut MF manual](#).
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Sites**.
4. Select the Site Server.
5. In the **Configuration** area, enter the IP address or DNS name of the PaperCut MF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

### 5.2 Security settings

#### 5.2.1 HTTPS Security (recommended)

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

**Note:** Until HTTPS is configured, the following warning is displayed on the PaperCut MF Admin web interface:



To enable HTTPS, you must have an SSL certificate installed on the PaperCut MF Application Server. The certificate must use the server's fully-qualified domain or IP address. This must be defined either in the **Common Name** (CN) field or included in the **Alternative Names** (AN) of the subject of the certificate. Without this, the device cannot connect to the server, since devices do not work with hostname-only certificates (i.e. not fully qualified).

You can use either **self-signed certificates** or **CA-signed, trusted certificates**:

- **Self-signed certificates** - If you are using the self-signed certificate that is generated by default when installing PaperCut MF, ensure to regenerate it for a fully qualified domain

name (or IP address). This is because the default self-signed certificate generated during PaperCut MF installation (device registration and integration) is issued using a hostname, instead of the IP address.

To use self-signed certificates:

1. Regenerate it using PaperCut MF's `create-ssl-keystore` tool in: `[PaperCut MF Install Location]\server\bin\[platform]`
  2. Run the following command to regenerate the certificate using the tool: `create-ssl-keystore -f "myserver.fullname.com"`  
For more information, see the [PaperCut MF manual](#).
  3. Set the config key `ext-device.hp-oxpd.use-ssl` to `Y`. For more information, see [5.13 Config Editor](#).
  4. It is recommended that you set the config key `ext-device.hp-oxpd.port-num` to `443`. For more information, see [5.13 Config Editor](#).
- **CA-signed, trusted certificates** - If you are using an official CA-signed certificate (for example, Verisign, Thawte), is likely to use the server's fully qualified domain name (or wildcard). This is because Certificate Authorities generally no longer accept certificate requests for either intranet names or IP addresses.

To use CA-signed, trusted certificates:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Certificate Management**.
3. In the **CA Certificates > Certificates** table, verify that the relevant Root and any required Intermediary Certificates are listed.

For example:

Issued To	Issued By	Expiration Date	Certificate Type	Certificate Usage
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>				
<input type="radio"/>	COMODO RSA Certification Authority	18 Jan, 2038 23:59:59	Root CA Certificate	
<input type="radio"/>	COMODO RSA Domain Validation Secure Server CA	11 Feb, 2029 23:59:59	Intermediate CA Certificate	

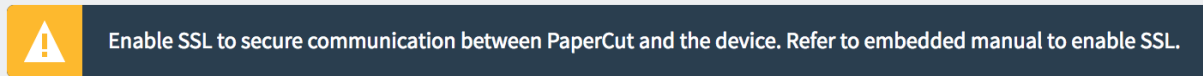
**Note:**

- If the relevant Root Certificate is not listed, click **Choose File**; select the relevant Root Certificate, click **Open**, and then click **Install**.
  - If the relevant Intermediary Certificate is not listed, click **Choose File**; select the relevant Intermediary Certificate, click **Open**, and then click **Install**.
4. Set the config key `ext-device.hp-oxpd.use-ssl` to `Y`. For more information, see [5.13 Config Editor](#).
  5. It is recommended that you set the config key `ext-device.hp-oxpd.port-num` to `443`. For more information, see [5.13 Config Editor](#).

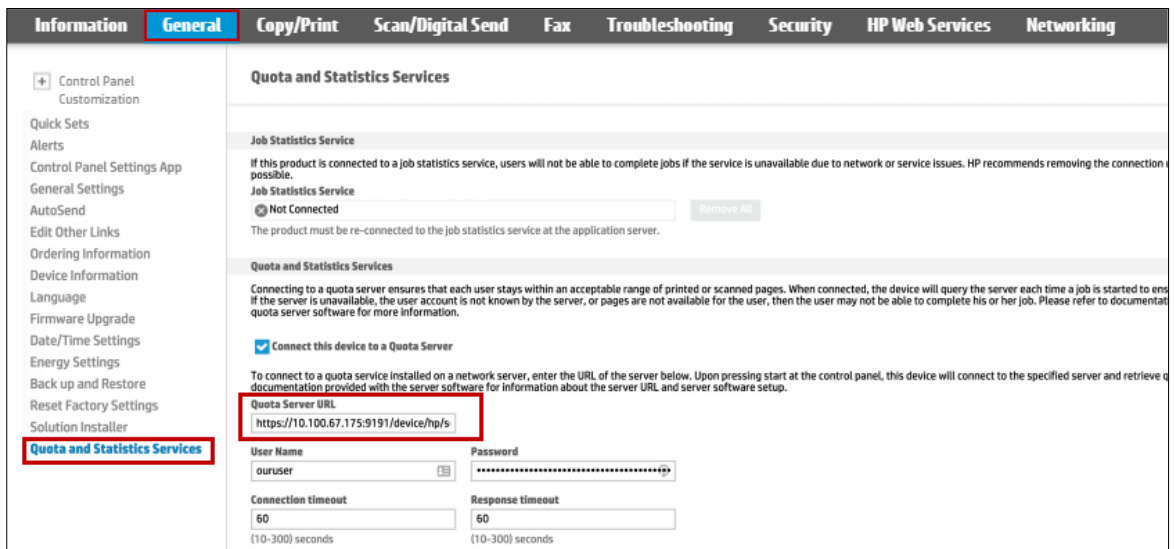
**Note:** After attempting to enable HTTPS, if the **Device Status** displays **Started (with errors) – Unknown error**, then see [8.5 Device Status "Started \(with errors\) – Certificate error"](#).

To test HTTPS:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. Verify that the following warning message is not displayed:



5. Log in to the device's web interface as an administrator.
6. Navigate to **General > Quota and Statistics Services**.
7. Verify that **Quota Server URL** displays the URL as HTTPS



8. Verify that you are able to log in to the device as a test user (simple test user).
9. Log in to the device's web interface as an administrator.

### 5.2.2 Additional network security (optional)

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

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

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

## 5.3 Authentication methods

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 authentication methods are in the **Device Details** page's **External Device Settings** area:

**Access methods**

**User authentication**

Username and password

Identity number

Swipe card

**Guest access**

Allow guest/anonymous access

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

You may customize the default message on the first non-PaperCut MF device screen with instructions to help users access the device, based on the authentication methods selected.

For more information, see [5.10 Device's first screen's message](#).

The available authentication methods are:

Authentication Method	Description
<b>Username and password</b>	<p>This is the default authentication method.</p> <p>With this method, users use their domain/network username and password.</p>
<b>Identity number</b>	<p>With this method, users use their ID number. For more information, see the <a href="#">PaperCut MF manual</a>.</p> <p><b>Require PIN:</b> With this method, users use their id number and the PIN associated with the id number.</p> <p><b>Note:</b> 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.</p>



---

## 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 [5.4 "Swipe card" authentication method](#).

**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. You may use the config keys: **ext-device.card-self-association.use-secondary-card-number** and **ext-device.self-association-allowed-card-regex**. For more information, see [5.13 Config Editor](#).

**Configure HP Universal USB Proximity Card Reader (P/N:X3D03A):** If you use the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader, then you must select this. You must configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader to read the card types being used. For more information, see [5.4.2 HP Universal USB Proximity Card Reader \(Part Number X3D03A\) or RF IDEas RDR-805H3AKU Card Reader](#). With this method, users use their registered swipe card on the configured HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader.

---

## Allow guest/anonymous access

With this method, you may choose to activate **guest** or **anonymous access**, enabling users to be authenticated as a guest user or an anonymous user, as per the user specified in the **Inherit settings from user** field.

**Inherit settings from user:** Enter the username of the PaperCut MF user's profile that is used while authenticating users as a guest user or an anonymous user on the device.

- **Guest access** - Selecting **Allow guest/anonymous access** and also selecting one or more of the other options (Username

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

- A **Guest** button, which may be customized, is displayed on the PaperCut MF Login screen on the device, together with the other options selected.  
**Note:** To customize the text of the **Guest** button that appears on the PaperCut MF Login screen, use the config key **ext-device.hp-oxpd.guest-access.label**. For more information, see [5.13 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.
- This guest user is shown the PaperCut MF Account Confirmation screen only if the user profile of the user specified in the **Inherit settings from user** field is entitled with the option of account selection, irrespective of the **External Device Settings > Device Options > Show account confirmation** checkbox setting.
- **Anonymous access** - Only selecting **Allow guest/anonymous access** *without* selecting any other option, 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.

---

#### Description of available authentication methods

## 5.4 "Swipe card" authentication method

If the **Swipe card** authentication method is selected, then the config key **ext-device.hp-oxpd.register.card-reader** is automatically set to **Y**, to allow PaperCut MF to register and establish an exclusive lock on card readers that are detected on the device. For more information, see [5.13 Config Editor](#).

### 5.4.1 Supported card readers

*PaperCut MF - HP OXP* supports the following configured and compatible card readers on HP FutureSmart 4 devices:

- Elatec TWN3 HID Prox
- Elatec TWN3 iCLASS
- Elatec TWN3 Mifare
- Elatec TWN4 Mifare
- HP Proximity Reader (CZ208A)
- HP Proximity Reader (CE931A)
- HP Proximity Reader (CE983A)
- HP Universal USB Proximity Card Reader (Part Number X3D03A)
- RF IDEas RDR-805H1AKU
- RF IDEas RDR-805H3AKU
- RF IDEas RDR-805T1AKU
- RF IDEas RDR 80581AKU-PPCT
- Securakey ET4-AUS-D

**Note:** In addition to the above card readers, you may customize *PaperCut MF - HP OXP* to support other card readers on HP FutureSmart 4 devices by using the config key **ext-device.hp-oxpd.additional-card-readers.vid-pid.hex**. For more information, see [5.13 Config Editor](#).

### 5.4.2 HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader

If the **Swipe card** authentication method is selected and you are using the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader, then you must configure it to read the card types being used. This is because your card reader's existing configurations are cleared and reset during PaperCut MF installation (device registration and integration).

To configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDEas RDR-805H3AKU Card Reader on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In the **External Device Settings**, select the **Swipe card** user authentication access method:

### External Device Settings

Allows for the configuration of the external device. For example connection settings like IP addresses and ports.

**Device type**  
HP (FutureSmart)

**Device's administrator username**

**Device's administrator password**

**Access methods**

**User authentication**

Username and password

Identity number

Swipe card

5. Select **Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)**.

Require PIN

Enable self-association with existing user accounts

**Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)**

**Card type #1**

**Card type #2**

**Card type #3**

**Card type #4**

6. Select the card type to be read by your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU card reader:

**Card type #1**

-- Not Configured --

- Farpointe Data UID
- Farpointe Data (Pyramid) PSC-1 26 Bit
- FeliCa
- HID iClass CSN
- HID iClass ID
- HID Prox
- HID Prox UID
- HiTag 1 and S (RDR-6H8x Compatible)
- HiTag 1 and S Alternate
- HiTag 2 (RDR-6H8x Compatible)
- HiTag 2 Alternate
- Gprox-II ID
- Gprox-II UID (HP)
- GProx-II UID (RDR-6G8x Compatible)
- I-Code CSN (Philips, NXP)
- I-tag CSN (IBM)
- iClass CSN, ISO1443A CSN, ISO15693A CSN (RDR-758x Compatible)
- ID Teck (RDR-6A8x Compatible)
- ID Teck Alternate
- Indala ASP 26 Bit (Motorola)

- You can configure up to four card types:

**Card type #1**

MiFare Ultralight CSN (Philips, NXP)

---

**Card type #2**

HID Prox

---

**Card type #3**

FeliCa

---

**Card type #4**

HiTag 2 Alternate

- If you are not using all four card types, select "--Not Configured--" for the unused card types.

<b>Card type #1</b>
MiFare Ultralight CSN (Philips, NXP) ▼
<b>Card type #2</b>
HID Prox ▼
<b>Card type #3</b>
-- Not Configured -- ▼
<b>Card type #4</b>
-- Not Configured -- ▼

- Some card types conflict with other card types. Hence, avoid selecting such conflicting card types, because this causes some problems if using swipe card authentication for logging in and self-association. For more information, see [8.3 Swipe card authentication anomalies](#).

7. Click **Apply**.

8. Verify that your card reader can read the card types configured.

**Note:** Your card reader's configuration is reset and you must re-configure your card reader every time any one of the following occurs:

- your card reader is disconnected from and reconnected to your device's USB port
- your device is restarted
- your PaperCut MF Application Server is restarted
- your device's details are modified on the PaperCut MF Admin web interface's **Device Details** page

### 5.4.3 Methods of handling card identifiers

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

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

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

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

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

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

### 5.4.3.1 Regular expression filters

To extract card identifiers using regular expression filters, use the config keys **ext-device.self-association-allowed-card-regex** and **ext-device.card-no-regex**. For more information, see [5.13 Config Editor](#).

Some regular expression filters include:

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

For more information, see [www.regular-expressions.info](http://www.regular-expressions.info).

### 5.4.3.2 Standard format converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see [5.13 Config Editor](#).

Some examples of standard format converters are:

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

---

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

---

### 5.4.3.3 Custom JavaScript converters

To use a custom JavaScript converter:

1. Create a JavaScript file. For example:  
**[install-path]/server/custom/card.js**
2. Define a single JavaScript function in this file called **convert**. It must accept and return a single string. For example:  

```
function convert(cardNumber) {  
    return cardNumber.substring(3,10).toLowerCase();  
}
```
3. Include a converter in the form: **javascript:custom/card.js**
4. Optionally, include a JavaScript script in the pipeline. For example:  
**ascii-enc|hex2dec|javascript:custom/card.js**
5. Verify the JavaScript converter from the following log:  
**[install-path]/server/log/server.log**
6. Use the config key **ext-device.card-no-converter** to modify card identifiers using custom JavaScript converters. For more information, see [5.13 Config Editor](#).

## 5.5 Device functions

PaperCut MF supports several device functions on most devices. These include:

- [5.5.1 Device functions controlled and tracked by PaperCut MF](#)
- [5.5.2 Device functions not controlled and tracked by PaperCut MF](#)
- [5.5.3 Administrative device functions](#)

### 5.5.1 Device functions controlled and tracked by PaperCut MF

Device functions controlled and tracked by PaperCut MF include functions such as copying, scanning, faxing, and print release.

To customize which of these device functions all users are permitted to access on the device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In the **External Device Settings** area, select the following device functions that all users are permitted to access on the device:
  - **Track & control copying** – tracking and controlling of copying and USB printing
  - **Track & control scanning** – tracking and controlling of scanning
  - **Track & control faxing** – tracking and controlling of faxing
5. In the **Print Release** area, select **Enable print release** to enable Hold/ Release and Find Me/ Secure Printing on the device.



- a. 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. For more information on configuring the printer queue's Hold/Release Queue Settings, see the [PaperCut MF manual](#).

## 5.5.2 Device functions not controlled and tracked by PaperCut MF

Device functions that are not controlled and tracked by PaperCut MF include functions such as Load Fax Quick Set, Load Email Quick Set, Scan to SharePoint®.

You can customize access to these device functions using any of the following methods:

- [5.5.2.1 Using PaperCut MF to customize access to device functions](#)
- [5.5.2.2 Using the device's Access Control to customize access to device functions](#)

### 5.5.2.1 Using PaperCut MF to customize access to device functions

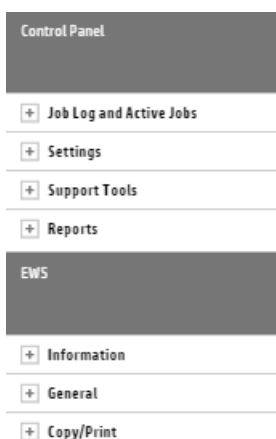
To use PaperCut MF to customize which of the device functions all authenticated users are permitted to access on the device, use the config key **ext-device.hp-oxpd.permission.whitelist**. For more information, see [5.13 Config Editor](#).

### 5.5.2.2 Using the device's Access Control to customize access to device functions

To use the device's Access Control to customize access to device functions:

1. Set the config key **ext-device.hp-oxpd.permission.server-managed** to **N**. For more information, see [5.13 Config Editor](#).
2. Log in to the device's web interface as an administrator.
3. Navigate to **Security > Access Control > Sign-In and Permission Policies**.

The **Control Panel** and **EWS** columns display rows of all device functions available on the device. These include administrative and non-administrative device functions, some of which are controlled and tracked by PaperCut MF, and some of which are not:



By default, the **Device Administrator** column enables all device function rows of the **Control Panel** and **EWS** columns, allowing all authenticated administrators to access all device functions:

Control Panel	Device Guest	Device Administrator	Device User	Sign-In Method
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	PaperCut MF
+ Job Log and Active Jobs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Use Default
+ Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Use Default
+ Support Tools	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Use Default

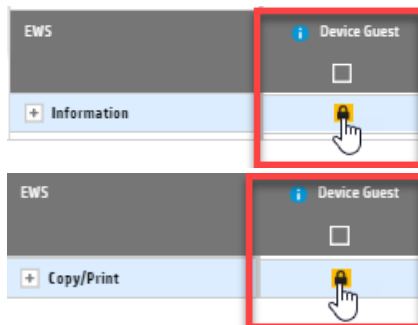
4. In the **Control Panel**, **Sign-In Method** column, select **PaperCut MF**:

Control Panel	Device Guest	Device Administrator	Device User	Sign-In Method
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	PaperCut MF

5. Using the **Device Guest** column, specify the device functions that require authentication and the ones that do not. It is recommended that all device functions that are tracked and controlled by PaperCut MF are accessible only to authenticated users.

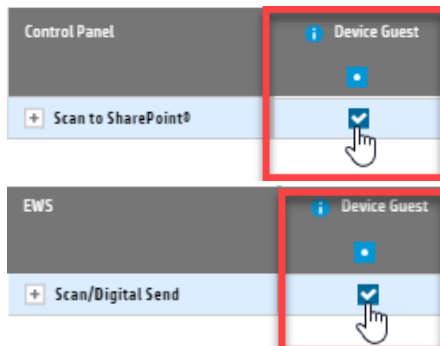
**Note:** This overrides any existing **Filters and Restrictions** that may be configured in the PaperCut MF Admin web interface for the device’s printer. For example, if the device’s Printer on the **Printers > Printer List > Printer Details > Filters & Restrictions** page, is enabled with **Groups With Color Access > Only allow the following groups to print in color** set to a specific group of users, but if the **Device Guest** column is enabled with **Print in color**, then all users are able to print in color.

- **Require authentication (Locked):** Lock the device function rows of the **Control Panel** and **EWS** columns that require authentication:



**Note:** It is recommended that **ALL** device function rows of the **Control Panel** and **EWS** columns are **locked**.

- **Do not require authentication (Ticked):** Tick the device function rows of the **Control Panel** and **EWS** columns that do not require authentication:

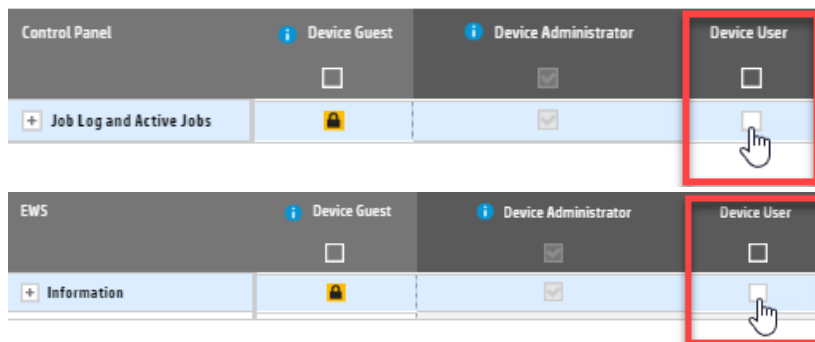


**Note:** It is recommended that **NO** device function rows of the **Control Panel** and **EWS** columns are **ticked**.

- Using the **Device User** column, specify the device functions that require administrative authentication and the ones that do not. It is recommended that all administrative device functions be accessible only to authenticated administrators.

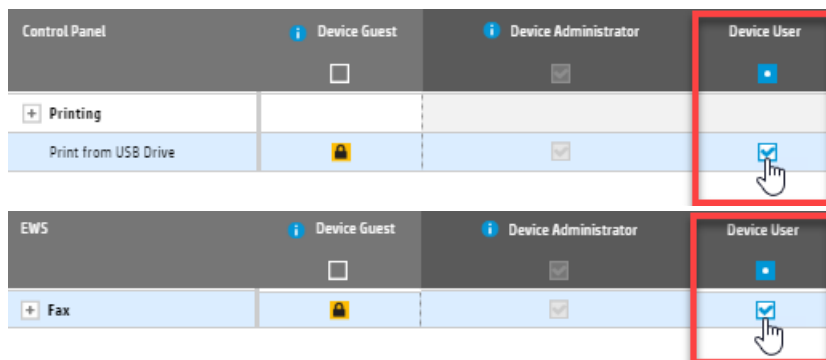
**Note:** This overrides any existing **Filters and Restrictions** that may be configured in the PaperCut MF Admin web interface for the device's printer. For example, if the device's Printer on the **Printers > Printer List > Printer Details > Filters & Restrictions** page, is enabled with **Groups With Color Access > Only allow the following groups to print in color** set to a specific group of users, but if the **Device User** column is enabled with **Print in color**, then all users are able to print in color.

- Require administrative authentication (Un-ticked):** Un-tick the device function rows of the **Control Panel** and **EWS** columns that require administrative authentication. These device functions appear with a lock icon and are unavailable to non-administrative users. For more information, see [8.6 Administrative device functions are unavailable to users](#).



**Note:** It is recommended that administrative device function rows of the **Control Panel** and **EWS** columns are **Un-ticked**.

- Do not require administrative authentication (Ticked):** Tick the device function rows of the **Control Panel** and **EWS** columns that do not require administrative authentication. These device functions are available to all authenticated users.



**Note:** It is recommended that *ONLY* non-administrative device function rows of the **Control Panel** and **EWS** columns are **Ticked**.

- Click **Apply**.

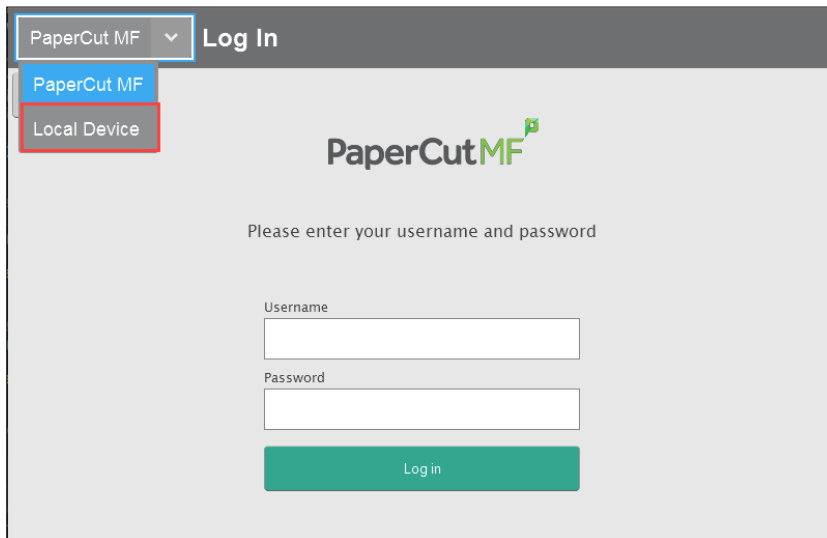
### 5.5.3 Administrative device functions

Administrative device functions include functions such as Supplies, Contacts, Reports, Settings, Support Tools, Job Log.

**Note:** By default, PaperCut MF locks certain administrative device functions on the device, making them available to administrators. For more information, see [8.6 Administrative device functions are unavailable to users](#). To change this default access permissions and restrictions, see [5.5.2.2 Using the device's Access Control to customize access to device functions](#).

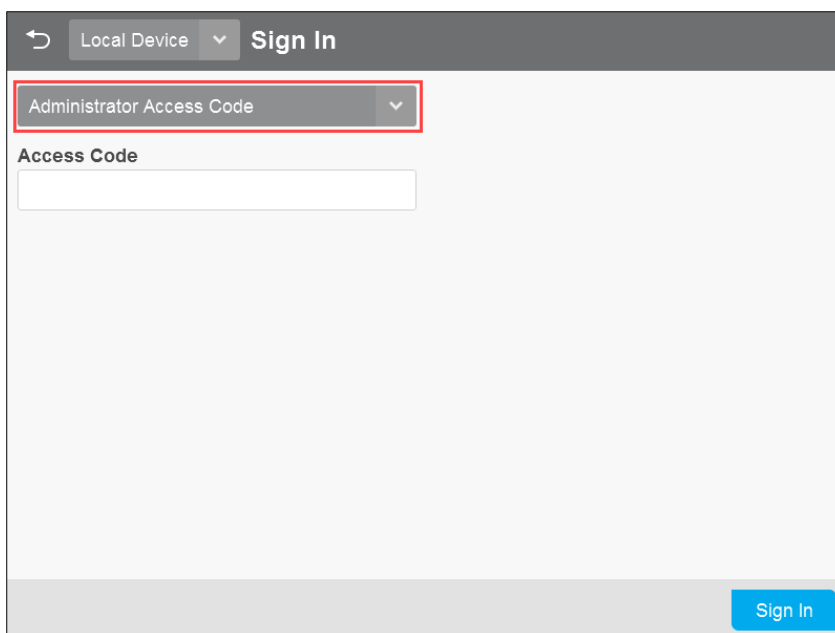
To access administrative device functions on the device as an administrator:

1. Navigate to the PaperCut MF Login screen on the device.
2. Select **Local Device**:



The screenshot shows the PaperCut MF Login interface. At the top left, there is a dropdown menu with 'PaperCut MF' selected. Below it, a list of options is shown: 'PaperCut MF' (highlighted with a blue box) and 'Local Device' (highlighted with a red box). The main area of the screen features the PaperCut MF logo, the text 'Please enter your username and password', and two input fields labeled 'Username' and 'Password'. A green 'Log in' button is positioned below the input fields.

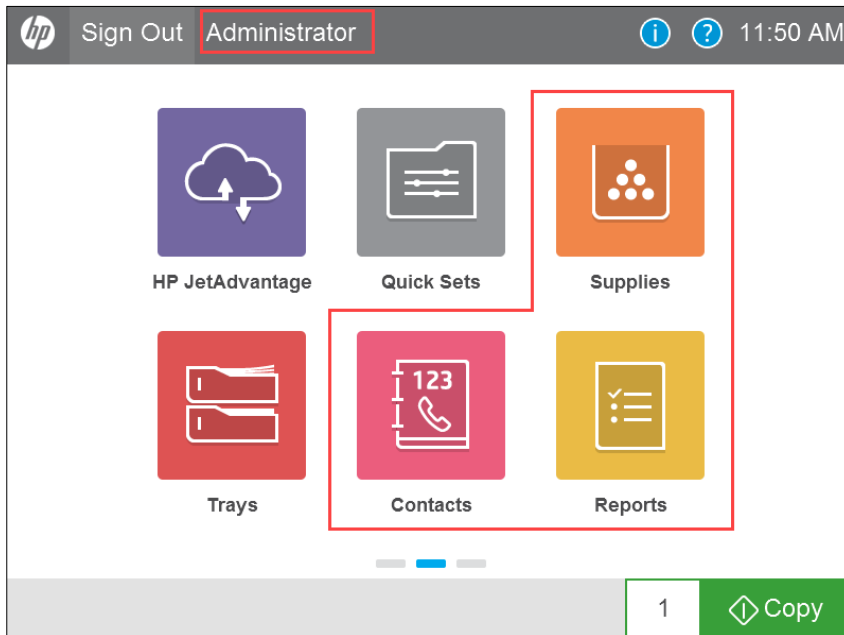
3. Select **Administrator Access Code**:



The screenshot shows the PaperCut MF Sign In interface. At the top left, there is a dropdown menu with 'Local Device' selected. Below it, a list of options is shown: 'Administrator Access Code' (highlighted with a red box). The main area of the screen features the text 'Access Code' and a large input field. A blue 'Sign In' button is located at the bottom right of the screen.

4. In **Access Code**, enter the administrator credentials (password) used for the device's web interface. For more information, see [3.3.1 Log in to the device web interface](#).
5. Click **Sign In**.

6. Select the relevant administrative device function (such as, Supplies):



7. For more information about each administrative function, consult the applicable third-party documentation available.

## 5.6 Held print jobs settings at the device

PaperCut MF allows you to configure the following:

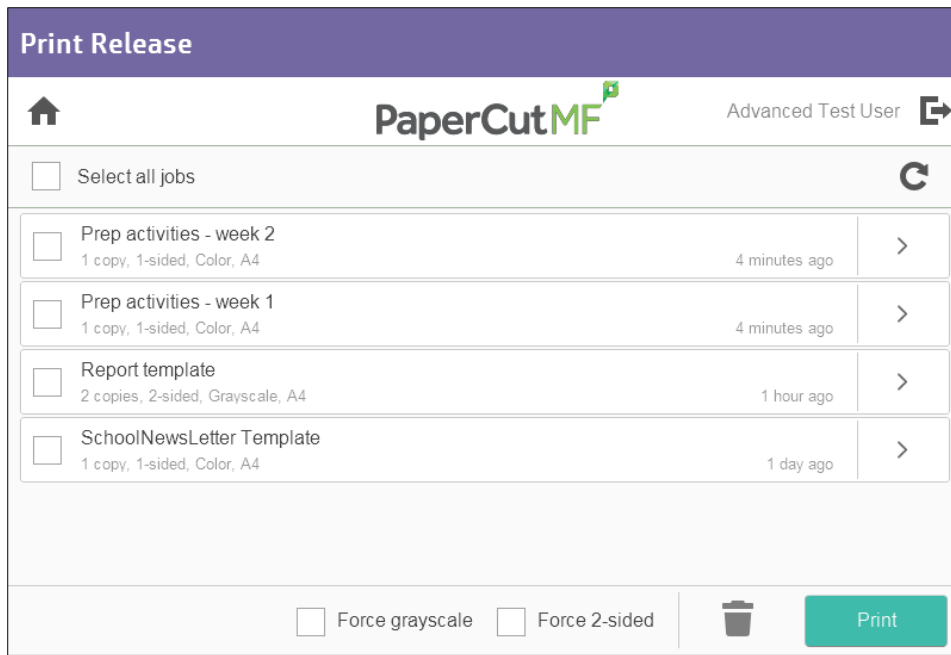
- [5.6.1 Held print jobs settings that can be changed at the device](#)
- [5.6.2 Held print jobs settings that can be viewed at the device](#)

### 5.6.1 Held print jobs settings that can be changed at the device

PaperCut MF allows users to change the settings of held print jobs on the device. Based on the changes made, PaperCut MF shows the updated cost and savings, to give immediate positive feedback to the user, encouraging behavior change.

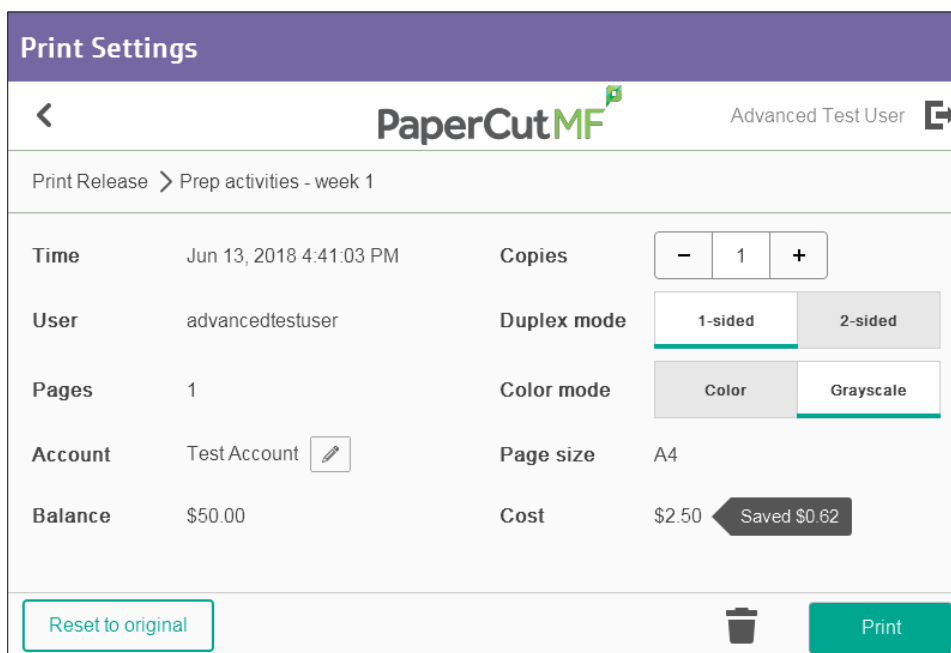
Users can make the following changes to print settings for multiple jobs on the device:

- **Force grayscale** (from color to grayscale)
- **Force 2-sided** (from 1-sided to 2-sided)



Clicking the chevron of a held print job displays all the settings for the individual job, allowing users to make the following additional changes:

- **Copies**
- **Duplex mode** (from 1-sided to 2-sided)
- **Color mode** (from color to grayscale)
- **Account**



If required, you can however, prevent users from being able to change print settings on the device. For more information, see the [PaperCut MF manual](#)

## 5.6.2 Held print jobs settings that can be viewed at the device

By default, PaperCut MF displays the following print settings for individual jobs on the device:

- **Account**
- **Balance**
- **Cost**

PaperCut MF also displays the total cost for multiple jobs on the device.

If required, you can however, prevent users from being able to view print settings on the device. For more information, see the [PaperCut MF manual](#)

## 5.7 Scanning

### 5.7.1 PaperCut MF's Integrated Scanning

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

1. Configure it on the PaperCut MF Admin web interface.  
For more information, see [Integrated Scanning](#) or the [PaperCut MF manual](#).
2. Use the config keys:
  - **ext-device.hp-oxpd.timeout.scan-prompt-send.secs**
  - **ext-device.hp-oxpd.timeout.complete-scan-job.secs**For more information, see [5.12 Timeouts](#), [5.13 Config Editor](#).

### 5.7.2 Device's "Scan to Email"

To enable users to use **Scan to Email** on the device, users' email addresses must already be configured while creating and configuring users in PaperCut MF (**Users > User List > User Details > Primary email**). After this is completed, you must also configure Scan to Email on the device's web interface.

To configure Scan to Email on the device's web interface:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Scan/Digital Send > Email Setup > Default Job Options**.
3. Select **Enable Scan to Email**.
4. In **Outgoing Email Servers (SMTP)**, enter the relevant details and click **Add**:

**Email Setup > Default Job Options**

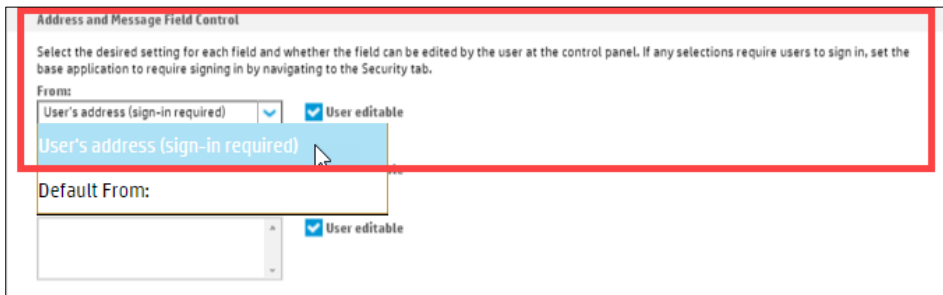
This feature allows users to scan documents and send them as email attachments to one or more email addresses.

**Enable Scan to Email**

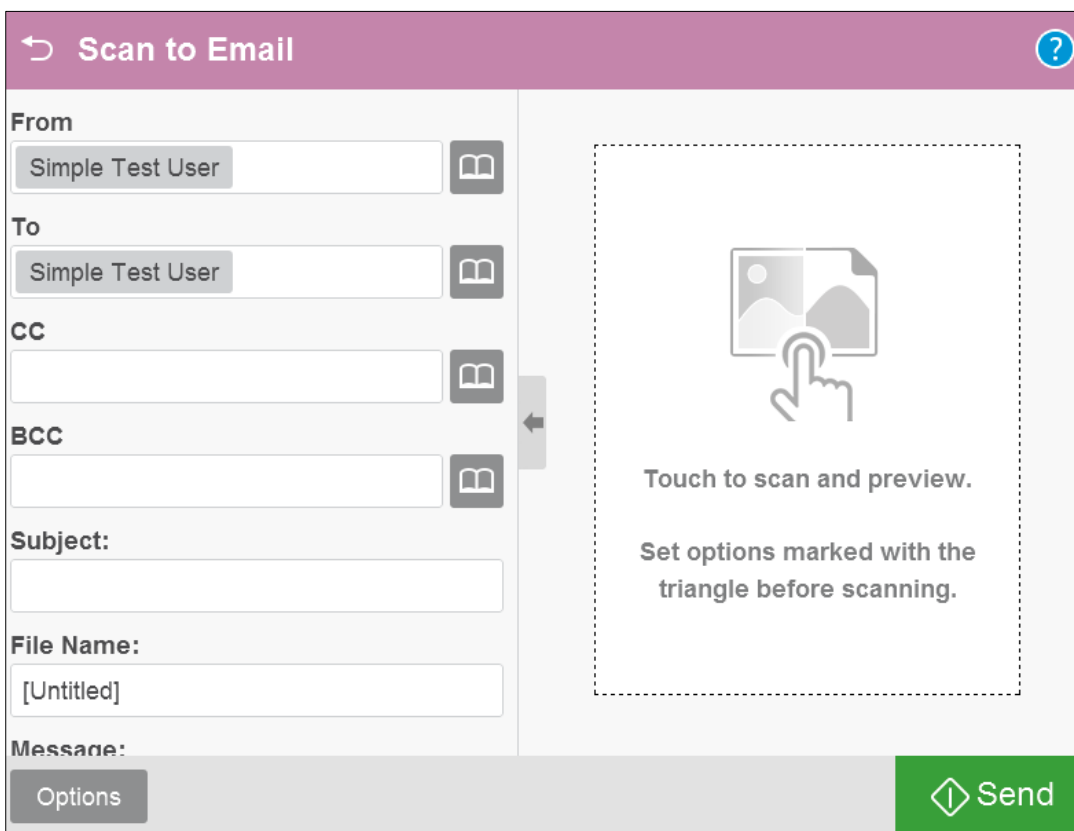
**Outgoing Email Servers (SMTP)**

Server Name	Port Number	Server Usage
10.100.64.203	5000	Send Email, Internet Fax, Automated Emails, AutoSend

- In the **Address and Message Field Control** area's **From** field, select **User's address (sign-in required)**:



- Click **Apply**.
- Log in to the device as a test user (simple test user).
- Verify that the **Scan to Email** screen's **From** and **To** fields display details of a test user (simple test user):



### 5.7.3 Device's "Scan to Network Folder"

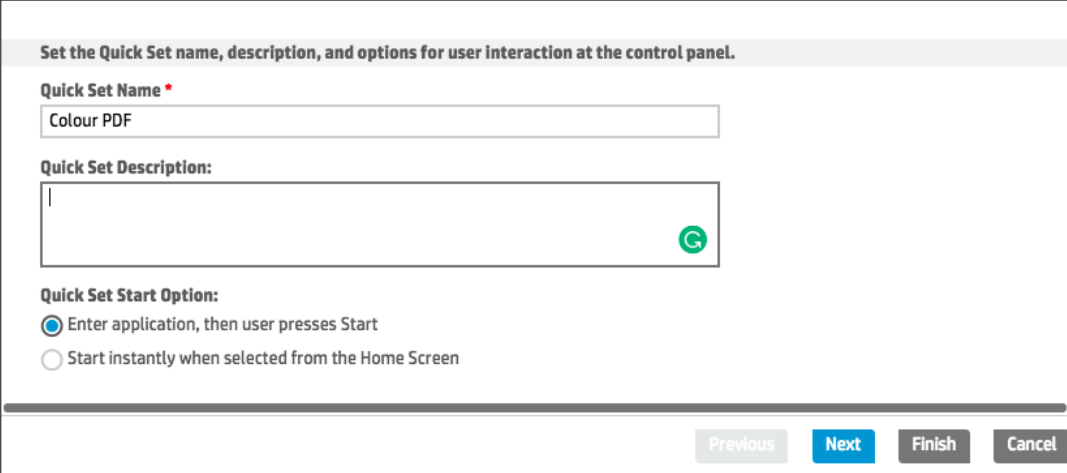
To enable users to use **Scan to Network Folder** on the device, you must configure Scan to Network Folder on the device's web interface. This is because the user home directory network path that is configured while creating and configuring users in PaperCut MF (**Users > User List > User Details > Home directory**) is *NOT* auto-populated on the device's **Scan to Network Folder > Folder Path**. For more information, see [6.4 The configured user home directory network path is not auto-populated on the device's Scan to Network Folder](#).

To configure Scan to Network Folder on the device's web interface:

- Log in to the device's web interface as an administrator.

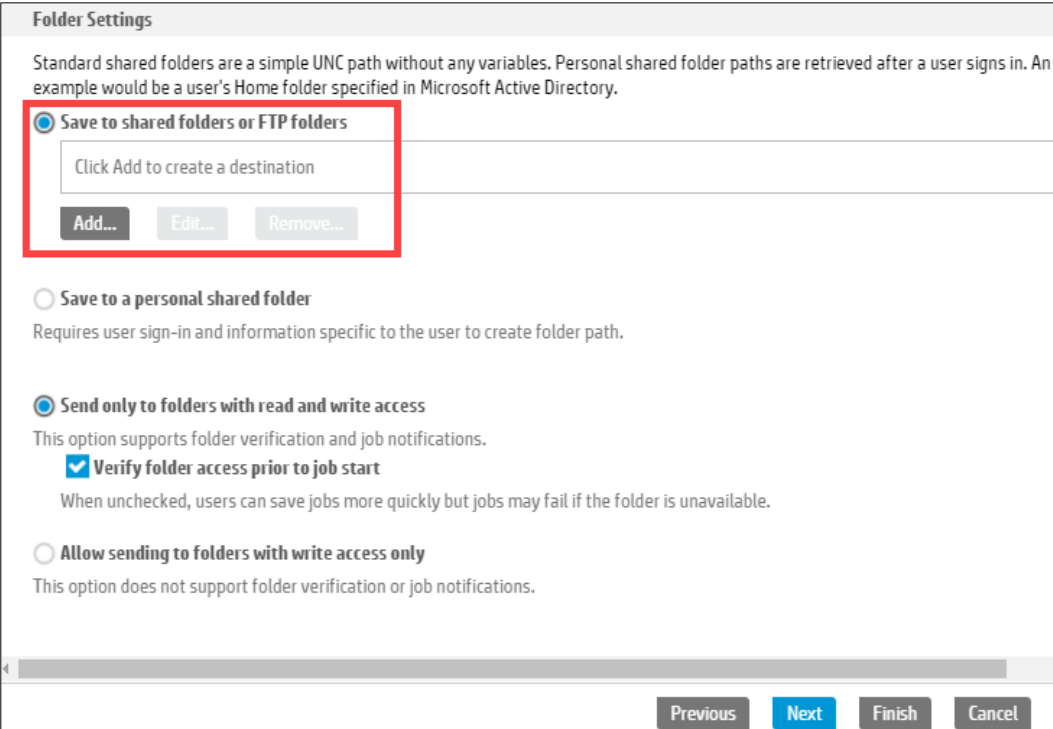


2. Navigate to **Scan/Digital Send > Scan to Network Folder > Default Job Options.**
3. Select **Enable Scan to Network Folder.**
4. Click **Apply.**
5. Navigate to **Quick Sets.**
6. Click **Add.**
7. Follow the **Quick Sets Wizard's** prompts:
  - a. In **Quick Set Name** enter a relevant name; click **Next**:



The screenshot shows a configuration window titled "Set the Quick Set name, description, and options for user interaction at the control panel." It contains three main sections: "Quick Set Name" with a text input field containing "Colour PDF"; "Quick Set Description" with a larger text area and a green circular icon; and "Quick Set Start Option" with two radio buttons: "Enter application, then user presses Start" (selected) and "Start instantly when selected from the Home Screen". At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

- b. In **Folder Settings**, select **Save to shared folders or FTP folders**; click **Add**:



The screenshot shows a configuration window titled "Folder Settings" with a descriptive paragraph about UNC paths. It features four radio button options: "Save to shared folders or FTP folders" (selected and highlighted with a red box), "Save to a personal shared folder", "Send only to folders with read and write access" (selected), and "Allow sending to folders with write access only". The "Send only to folders with read and write access" option has a checked checkbox for "Verify folder access prior to job start". Below the radio buttons is a text input field with the placeholder "Click Add to create a destination" and three buttons: "Add...", "Edit...", and "Remove...". At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

**Note:** Do *NOT* select and configure the **Save to a personal shared folder** option.

- c. Select **Save to a Standard shared network folder** and in **UNC Folder Path** enter the relevant directory's network path:

**Save to a standard shared network folder**

**UNC Folder Path:** \*

(\\path\path)

- d. Optionally, in the **Custom Subfolder** select the relevant option that is to be appended to the **UNC Folder Path**; to apply further access restrictions, select **Restrict subfolder access to user**:

**Custom Subfolder:**

+

Appends a custom subfolder at end of the folder path.

**Restrict subfolder access to user**

- e. Click **Update Preview**.
- f. Verify that the **Folder Path Preview** displays both the **UNC Folder Path** and the value of the **Custom Subfolder** (if configured):

**Edit Network Folder Path**

**Save to a standard shared network folder**

**UNC Folder Path:** \*

(\\path\path)

**Custom Subfolder:**

+

Appends a custom subfolder at end of the folder path.

**Restrict subfolder access to user**

**Folder Path Preview:**

**Update Preview**

Some Custom Subfolder values will be updated only when the Quick Set is used.

- g. In **Authentication Settings**, select **Always use these credentials**:

**Authentication Settings:**

- h. Enter the relevant details in **Windows Domain**, **User Name**, **Password**:

**Windows Domain:**

**User Name:**

**Password:**

- i. Click **Verify Access**:

- j. Click **Ok**.
- k. Verify that **Folder Settings > Save to shared folders or FTP folders > Network Folder Path** displays the configured **UNC Folder Path** and **Custom Subfolder** (if configured); click **Next**:

- l. In **Notification** select and configure the relevant notification; click **Next**:

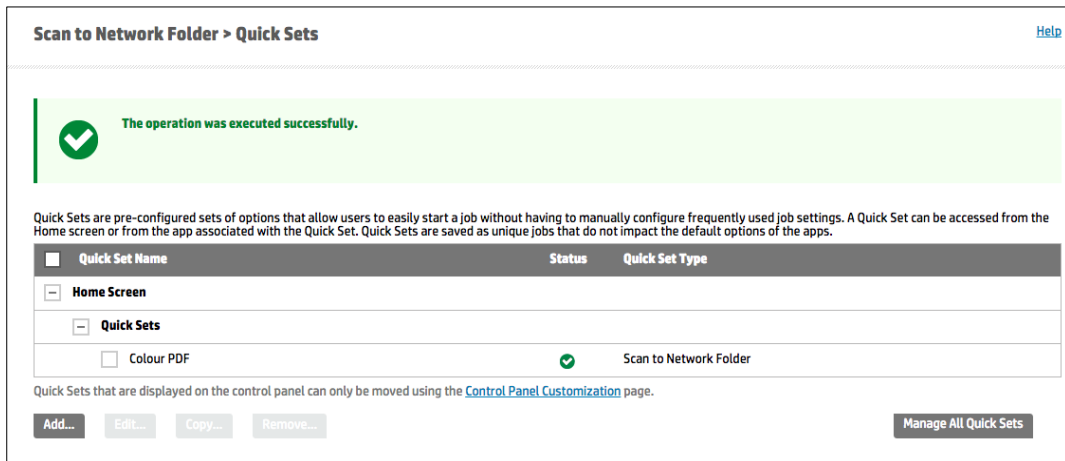
m. In **Scan Settings** select and configure the relevant scan settings; click **Next**:

n. In **File Settings** select and configure the relevant scan settings; click **Next**:

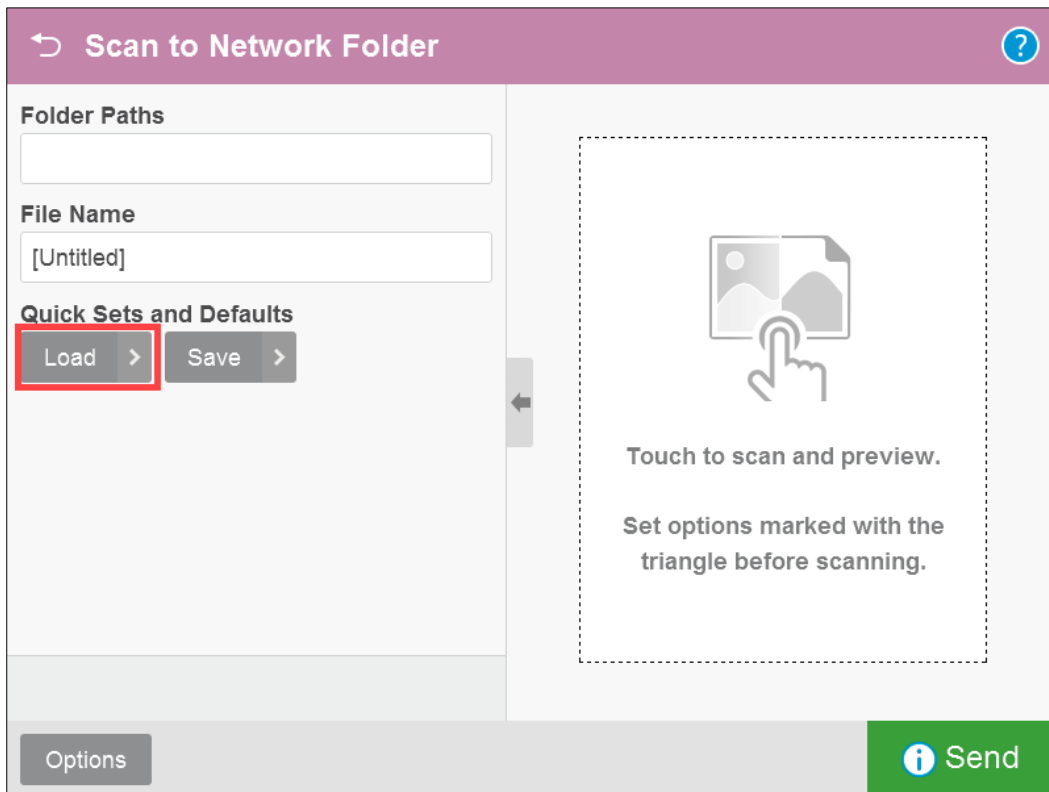
o. Verify that the **Summary** displays the summary of the configured Quick Set; click **Finish**:

8. Verify that on the **Scan/Digital Send > Scan to Network Folder > Quick Sets** page, the **Quick Set Name** is the name of the configured Quick Set, **Status** is a green tick icon, and **Quick Set**

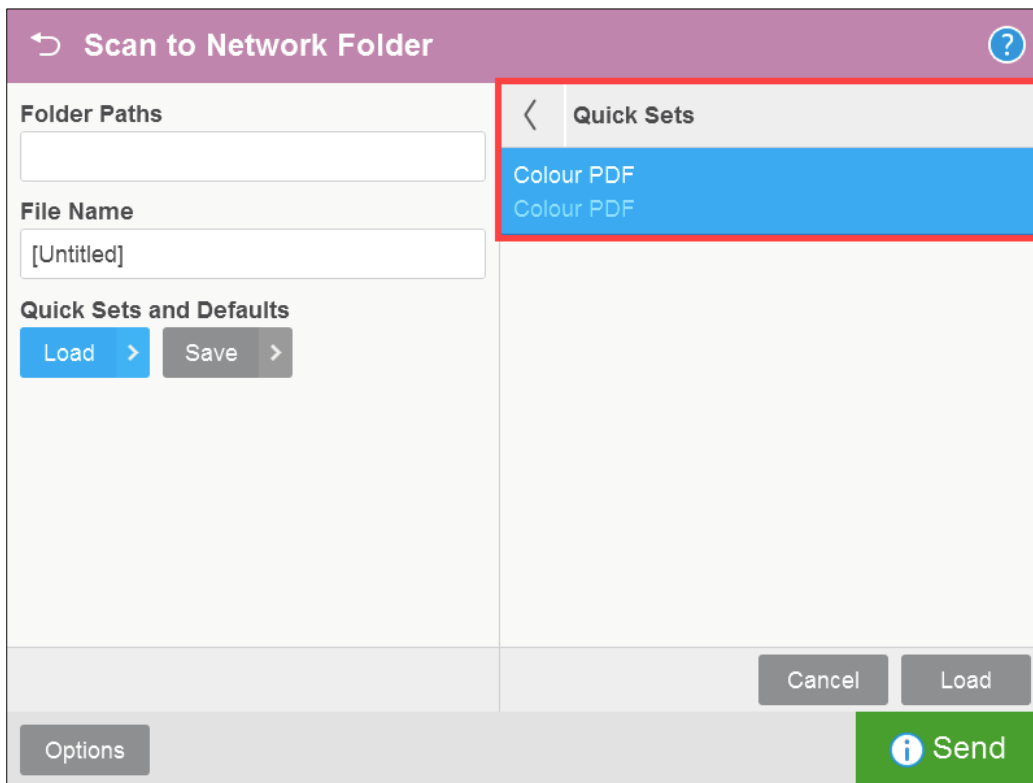
**Type is Scan to Network Folder:**



9. Log in to the device as a test user (simple test user).
10. On the **Scan to Network Folder** screen, click **Load**:

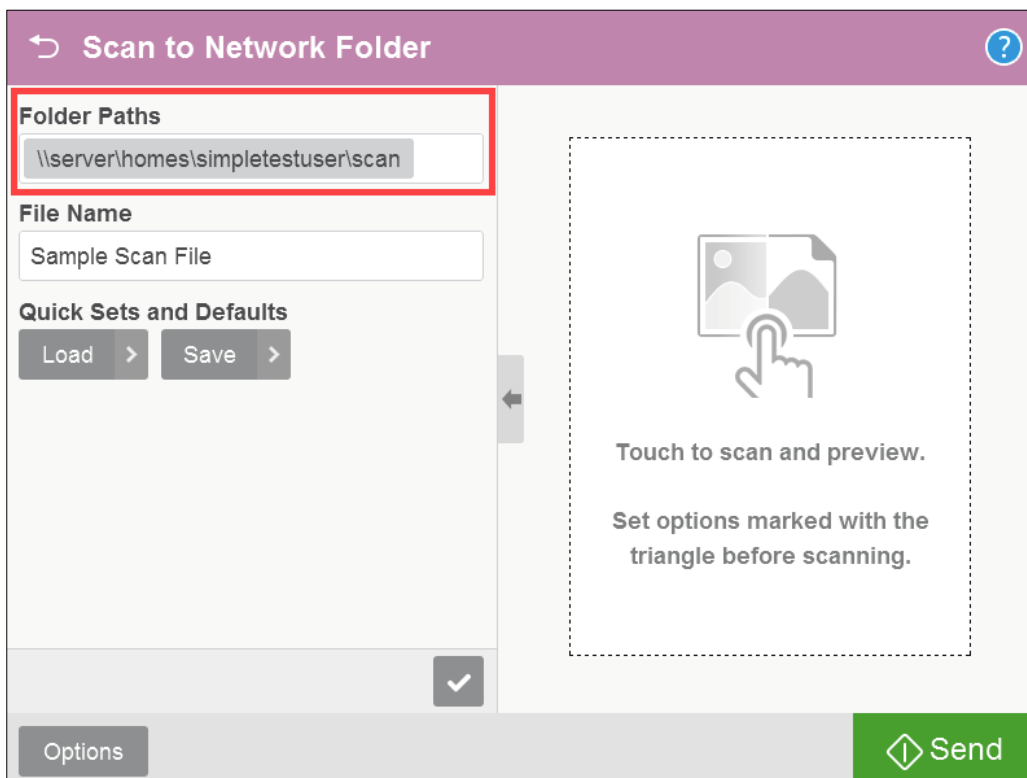


11. Verify that the **Scan to Network Folder** screen displays the configured Quick Set:



12. Select the **Quick Set** and click **Load**.

13. Verify that **Folder Path** displays the network path as configured in the device's web interface (**Scan/Digital Send > Scan to Network Folder > Quick Sets**):



## 5.8 Job charging

### 5.8.1 Job Limits and Zero Stop

PaperCut MF's Job Limits and Zero Stop features ensure that users are prevented from getting a negative balance, below the zero limit. PaperCut MF calculates a user's Job Limits by using the reference benchmarks specified in the following config keys, against the user's existing current balance and other restrictions:

- ext-device.hp-oxpd.limit-reference.duplex
- ext-device.hp-oxpd.limit-reference.grayscale
- ext-device.hp-oxpd.limit-reference.paper-size
- ext-device.hp-oxpd.restricted.multiple-txns

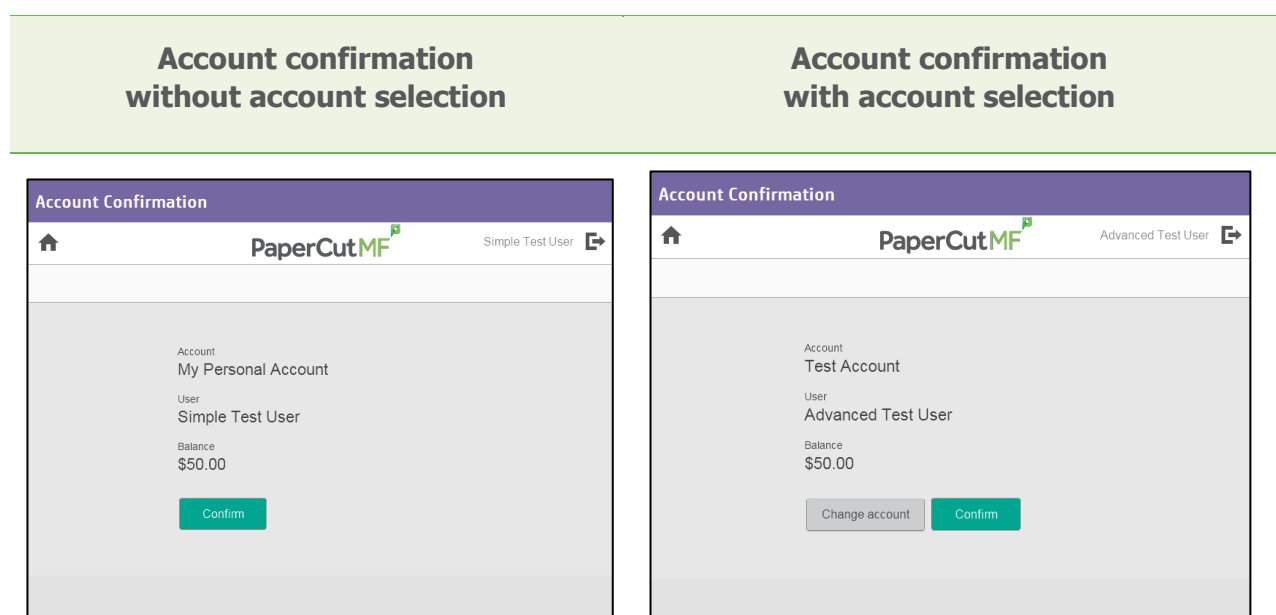
For more information, see [5.13 Config Editor](#).

However, since this calculation is based on configurable assumptions about the reference page (paper size, duplex or simplex attribute, and grayscale or color attributes), irrespective of the actual attributes of the user's job, it is possible for a restricted user to acquire a negative balance, if the references are configured more liberally. For example, if the config ext-device.hp-oxpd.limit-reference.paper-size is set to A3, but the user's job is an A4 job, then the user could run into a negative balance, if the final cost of the A4 job is more than PaperCut MF's initial calculation using the paper size reference configured as A3. By default, PaperCut MF's reference page is one, grayscale, single-sided A4 page.

Zero Stop also has some limitations with regard to USB printing, copying, scanning, and faxing. For more information, see [6.1 Zero Stop for USB printing is unavailable](#) and [6.2 The application of Zero Stop during copying or faxing is delayed](#).

### 5.8.2 Account confirmation

Based on whether a user has the option of account selection, the user is presented with one of the following PaperCut MF Account Confirmation screens on the device:



However, PaperCut MF also gives you the option of toggling the display of the PaperCut MF Account Confirmation screen on the device.

To access the PaperCut MF Account Confirmation screen's toggle on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. The PaperCut MF Account Confirmation screen's toggle is available through the **External Device Settings > Device Options > Show account confirmation** checkbox.

### 5.8.3 Account selection

The PaperCut MF Account Selection screen on the device allows users to select an account via any one of the following ways:

- [5.8.3.1 By name and by code](#)
- [5.8.3.2 By name](#)
- [5.8.3.3 By code](#)

This is based on a user's Account Selection setting on the PaperCut MF Admin web interface. To this on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Users**.
3. From the **User List**, select the user.
4. In the **Account Selection** area's **Print account selection**, select **Standard account selection popup** and in **Information to show in popup**, select all the options:

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

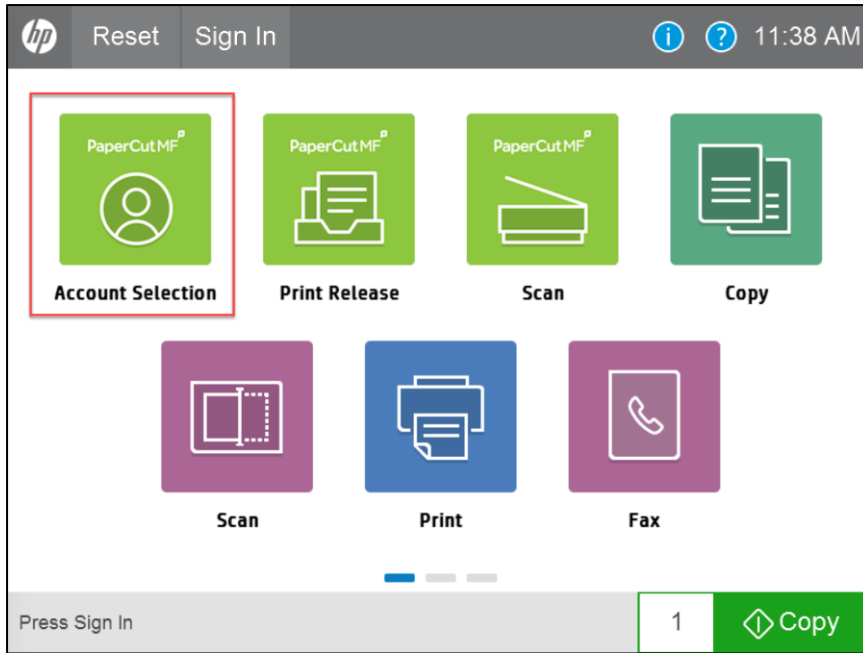
**Print account selection**  
Show the standard account selection popup

**Information to show in popup**

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

Once a user selects an account, the same account is used for subsequent transactions. However, users have the option of changing the account from the first screen on the device (the non-PaperCut MF device screen with the PaperCut MF icons), by selecting the **PaperCut MF Account Selection** icon:





**Note:** To toggle the display and availability of this **PaperCut MF Account Selection** icon, use the config key **ext-device.hp-oxpd.register.account-selection**. For more information, see [5.13 Config Editor](#).

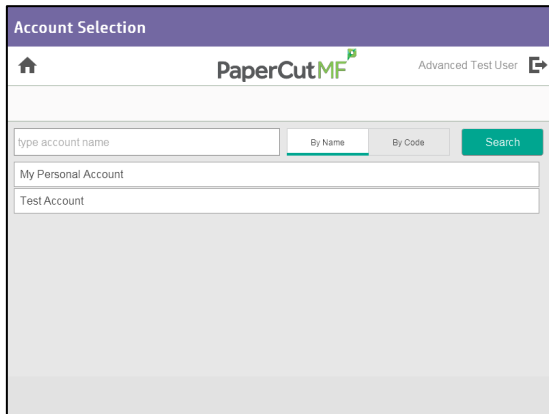
### 5.8.3.1 *By name and by code*

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to either of the following, the PaperCut MF Account Selection screen displays both methods of selecting accounts – by name and by code:

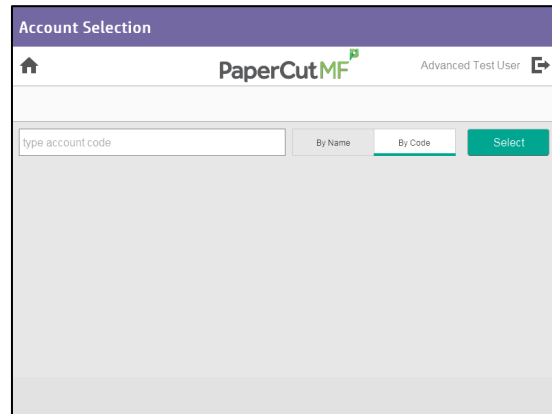
- **Show the advanced account selection popup, or**
- **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (from list)** and **Allow user to select shared accounts (using PIN/code)**

By Name	By Code
<p>Users select the relevant shared account by scrolling through a list of all applicable shared accounts (maximum of 100, with a scroll bar) or by searching for the shared account using the account’s name.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The user’s My Personal Account and the Default Shared Account (if set) is always displayed.</li> </ul>	<p>Users select the relevant shared account by using the shared account’s code.</p> <p><b>Note:</b> The user’s My Personal Account and the Default Shared Account (if set) is not displayed.</p>

- To customize the maximum number of applicable shared accounts displayed, use the config key **ext-device.hp-oxpd.account-list.limit**. For more information, see [5.13 Config Editor](#).



The screenshot shows the 'Account Selection' interface. At the top, there is a header with the PaperCut MF logo and 'Advanced Test User'. Below the header, there is a search bar labeled 'type account name' and two radio buttons: 'By Name' (selected) and 'By Code'. A 'Search' button is to the right. Below the search bar, a list of accounts is displayed, including 'My Personal Account' and 'Test Account'.



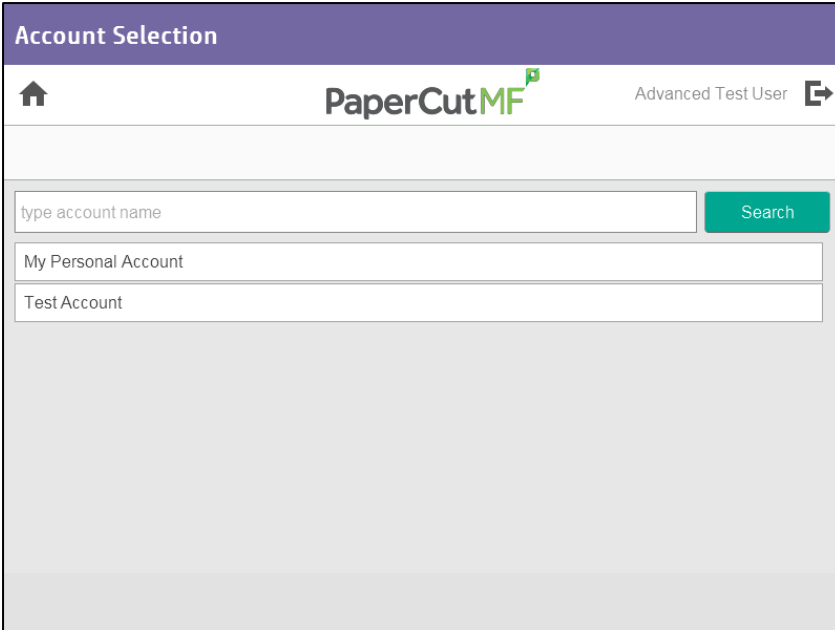
The screenshot shows the 'Account Selection' interface. At the top, there is a header with the PaperCut MF logo and 'Advanced Test User'. Below the header, there is a search bar labeled 'type account code' and two radio buttons: 'By Name' and 'By Code' (selected). A 'Select' button is to the right. The main area below is currently empty.

### 5.8.3.2 By name

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (from list)**, the PaperCut MF Account Selection screen displays only one method of selecting accounts – by name. Users select the relevant shared account by scrolling through a list of all applicable shared accounts (maximum of 100, with a scroll bar) or by searching for the shared account using the account's name.

**Note:**

- The user's My Personal Account and the Default Shared Account (if set) is always displayed.
- To customize the maximum number of applicable shared accounts displayed, use the config key **ext-device.hp-oxpd.account-list.limit**. For more information, see [5.13 Config Editor](#).

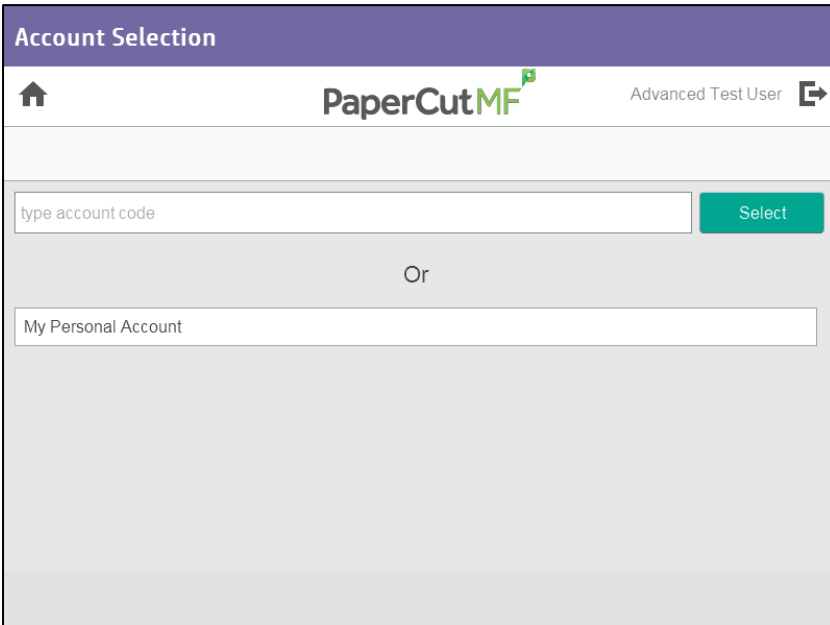


The screenshot shows the 'Account Selection' interface. At the top, there is a purple header with the title 'Account Selection'. Below the header is a navigation bar with a home icon, the 'PaperCutMF' logo, and the user name 'Advanced Test User' with an external link icon. The main content area features a search input field labeled 'type account name' and a green 'Search' button. Below the search field, a list of accounts is displayed: 'My Personal Account' and 'Test Account'.

### 5.8.3.3 By code

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (using PIN/code)**, the PaperCut MF Account Selection screen displays only one method of selecting accounts – by code. Users select the relevant shared account by using the shared account's code.

**Note:** The user's My Personal Account and the Default Shared Account (if set) is always displayed.



The screenshot shows the 'Account Selection' interface. At the top, there is a purple header with the title 'Account Selection'. Below the header is a navigation bar with a home icon, the 'PaperCutMF' logo, and the user name 'Advanced Test User' with an external link icon. The main content area features a search input field labeled 'type account code' and a green 'Select' button. Below the search field, the word 'Or' is centered. Below 'Or', a list of accounts is displayed: 'My Personal Account'.

## 5.9 Language and Keyboard Layouts

To configure the Language and Keyboard Layouts on the device's web interface:

1. Log in to the device's web interface as an administrator.

2. Navigate to **General > Control Panel Customization > Control Panel Language and Keyboard Layouts**.
3. Set the **Control Panel Language and Keyboard Layouts** fields as required.
4. Click **Apply**.

## 5.10 Device's first screen's message

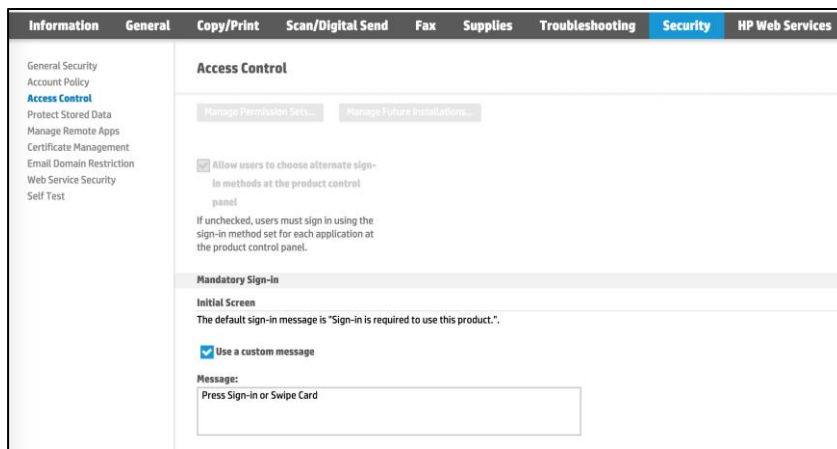
**Note:** This is applicable only if the device is running the **HP FutureSmart 4** platform's **Firmware Bundle Version 4.5.5**.

You may customize the default message on the first non-PaperCut MF device screen with instructions to help users access the device, based on the authentication methods selected. For more information, see [5.3 Authentication methods](#).

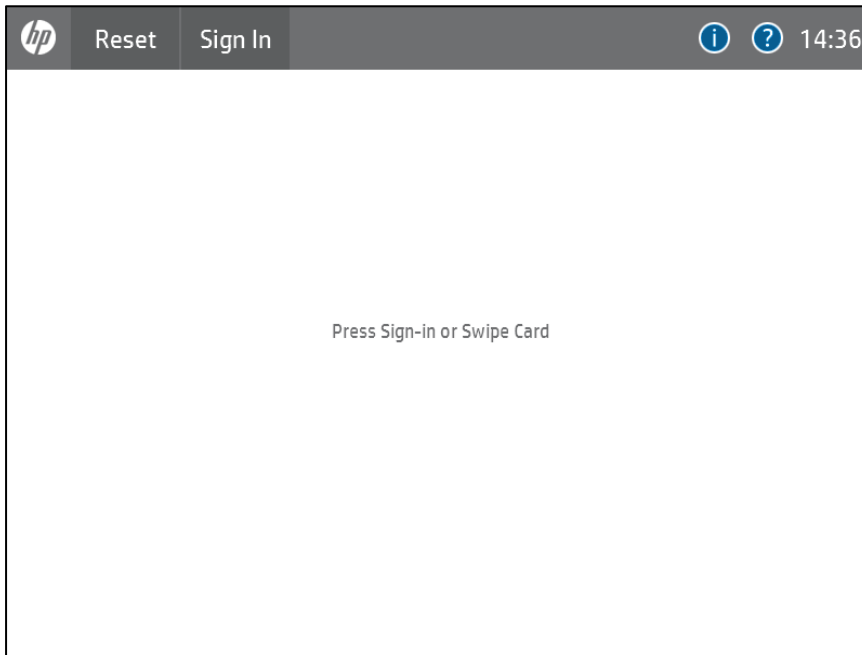
To customize the first non-PaperCut MF device screen's default message on the device's web interface:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Access Control**.
3. In **Mandatory Sign-In > Initial Screen**, select **Use a custom message**.
4. In **Message**, enter the message that appears on the first non-PaperCut MF device screen.

For example, instructions to help users access the device (either by clicking **Sign In** or by using their swipe cards, if the **Swipe card** authentication method is selected).



**Note:** This message appears on the first non-PaperCut MF device screen:



5. Click **Apply**.

## 5.11 Screen headers

### 5.11.1 Header colors

To customize the colors (background and text) of the headers on all PaperCut MF screens:

1. Use the following config keys:  
**ext-device.hp-oxpd.header.color**  
**ext-device.hp-oxpd.header.textcolor**  
For more information, see [5.13 Config Editor](#).
2. Log in to the device as a test user (simple test user).
3. Verify that the device's header background and text colors are as required.

### 5.11.2 Header logo

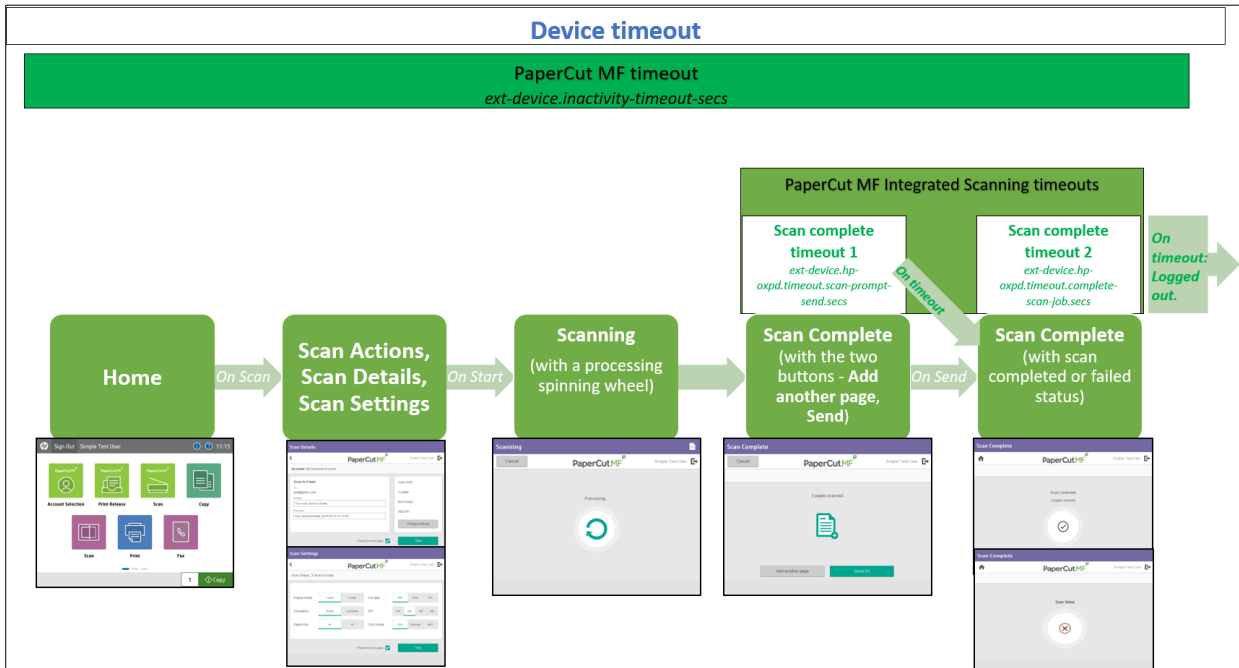
To customize the logo on the headers of all PaperCut MF screens:

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

## 5.12 Timeouts

A logged-in user who is detected as being idle (on a PaperCut MF screen or a non-PaperCut MF device screen) is automatically logged out after a certain interval of time, based on the following conditions:

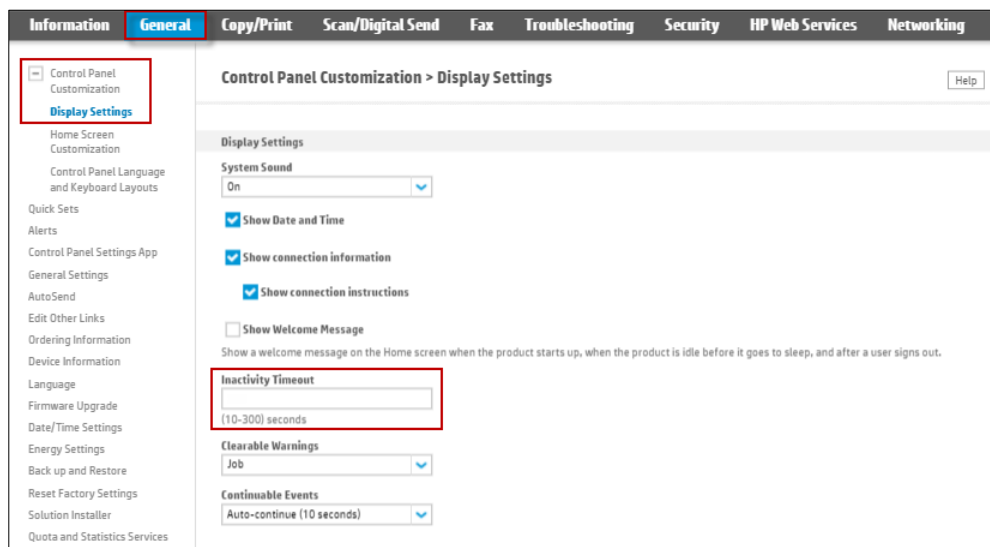
A user who is detected as being idle (on a PaperCut MF screen or a non-PaperCut MF device screen) is automatically logged out after a certain interval of time, based on the following conditions:



- **Device timeout** - If the user is idle on a non-PaperCut MF device screen, then the user is logged out based on the device's timeout.

To configure the device's timeout on the device's web interface:

- Log in to the device's web interface as an administrator.
- Navigate to **General > Control Panel Customization > Display Settings**.
- In **Inactivity Timeout**, enter the required device timeout.



**Note:** If the logged-in user is idle on a non-PaperCut MF device screen, then the user is logged out based on this value. However, if the logged-in user is idle on a PaperCut MF screen and if this value is lower than the PaperCut MF timeout (the config key **ext-device.inactivity-timeout-secs**), then the user is logged out based on this value (i.e. this value supersedes and overrides the higher value of the config key). For more information, see [5.12 Timeouts](#) and [5.13 Config Editor](#).

d. Click **Apply**.

- **PaperCut MF timeout** - If the logged-in user is idle on a PaperCut MF screen, then the user is logged out based on the config key **ext-device.inactivity-timeout-secs** or the device's timeout, whichever has the lower value. For more information, see [5.13 Config Editor](#).
- **PaperCut MF integrated scanning timeouts** – If the user is using Integrated Scanning, then timeouts are based on the following config keys:
  - **PaperCut MF scan complete timeout 1** - ext-device.hp-oxpd.timeout.scan-prompt-send.secs
  - **PaperCut MF scan complete timeout 2** - ext-device.hp-oxpd.timeout.complete-scan-job.secs

For more information, see [5.13 Config Editor](#)

## 5.13 Config Editor

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

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

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Actions > Config editor (advanced)**.

**Note:** For more information, see the [PaperCut MF manual](#).

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

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

The available config keys are:

Config name	Description
<b>Device screens</b>	

---

<b>ext-device.hp-oxpd.login-instruction</b>	<p>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.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none"><li>• Values: Any text, DEFAULT</li><li>• Default: DEFAULT (device-specific PaperCut MF text)</li></ul> <p><b>Note:</b> To add a line break, use <code>\n</code>. For example, <i>PaperCut Software\nSwipe your card to log in.</i></p>
---	---

---

<b>ext-device.hp-oxpd.guest-access.label</b>	<p>Customize the text of the <b>Guest</b> button that appears on the PaperCut MF Login screen.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none"><li>• Values: Any text, DEFAULT</li><li>• Default: DEFAULT (Guest)</li></ul> <p><b>Note:</b> This is applicable only if <b>guest access</b> is activated (<b>Allow guest/anonymous access</b> is selected and at least any one other option is also selected). For more information, see <a href="#">5.3 Authentication methods</a>.</p>
--	--

---

<b>ext-device.hp-oxpd.header.color</b>	<p>Customize the background color of headers on all PaperCut MF screens.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none"><li>• Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT</li><li>• Default: DEFAULT (dark green)</li></ul> <p><b>Note:</b> For more information, see <a href="#">5.11.1 Header colors</a>.</p>
--	---

---

<b>ext-device.hp-oxpd.header.textcolor</b>	<p>Customize the text color of headers on all PaperCut MF screens.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none"><li>• Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT</li><li>• Default: DEFAULT (white)</li></ul> <p><b>Note:</b> For more information, see <a href="#">5.11.1 Header colors</a>.</p>
--	--

---



---

**ext-device.hp-oxpd.release-show-cost**

Toggle the display of the cost of held print jobs on the PaperCut MF Print Release and Print Settings screens on the device.

This is a device-specific config key.

- Values: Y, N
- Default: Y

**Note:** Setting this to N also hides the account balance and does not display the savings based on other changes made to held print job settings. For more information, see [5.6 Held print jobs settings at the device](#).

---

**ext-device.hp-oxpd.register.account-selection**

Toggle the display of the **PaperCut MF Account Selection** icon on the device screen (the non-PaperCut MF device screen with the PaperCut MF icons).

This is a device-specific config key.

- Values: Y, N
- Default: Y

**Note:** For more information, see [5.8.3 Account selection](#).

---

**ext-device.hp-oxpd.account-list.limit**

Customize the maximum number of applicable shared accounts displayed on the PaperCut MF Account Selection screen.

This is a device-specific config key.

- Values: 1-500
- Default: 100

---

**ext-device.hp-oxpd.permission.whitelist**

Customize which of the device functions (not tracked and controlled by PaperCut MF), all authenticated users are permitted to access on the device.

This is a device-specific config key.

- Values: \* (all the following device functions), any one or a comma-separated combination of the following device functions (not case sensitive):
  - Copy
  - Copy/Print
  - Scan
  - USB Drive
  - Network Folder

- Email
- Scan to USB Drive
- Scan to Job Storage
- Scan to Network Folder
- Scan to SharePoint®
- Print from Job Storage
- Print from USB Drive
- Print in color
- Scan/Digital Send
- Ability to edit the network folder path
- Load Scan to Network Folder Quick Set
- Load Scan to USB Drive Quick Set
- 1-sided copy output
- Make a Color Copy
- Load Copy Quick Set
- Fax
- Load Fax Quick Set
- Ability to edit the From field for email
- Ability to edit the To field for email
- Ability to edit the CC field for email
- Ability to edit the BCC field for email
- Ability to edit the Subject field for email
- Ability to edit the body of an email
- Load Email Quick Set
- Default: \* (all the above device functions)

**Note:** This is not an exhaustive list of all device functions, device capabilities, third-party applications, and administrative device functions that are available on the device. For all devices functions that are available on the device see the following:

- the log file located in: [PaperCut MF Install Location]\server\logs\hp-oxp-installed-apps.log
- the device's Access Control settings. For more information, see [5.5.2.2 Using the device's Access Control to customize access to device functions](#).

---

**ext-device.hp-oxpd.permission.server-managed**

Enable or disable the use of PaperCut MF to customize access to device functions.

This is a device-specific config key.

- Values: Y, N
-

- Default: Y

**Note:**

- Setting this to Y – enables the use of PaperCut MF to customize access to device functions. This requires to configure the config key **ext-device.hp-oxpd.permission.whitelist**. For more information, see [5.5.2.1 Using PaperCut MF to customize access to device functions](#).
- Setting this to N – disables the use of PaperCut MF to customize access to device functions. This requires you to configure the device's Access Control settings. For more information, see [5.5.2.2 Using the device's Access Control to customize access to device functions](#).

---

**ext-device.hp-oxpd.scan.prompt.checkbox.checked**

Customize 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 Complete (with the two buttons - **Add another page, Send**) screen.

This is a device-specific config key.

- Values: Y (checked by default; can be changed by the user), N (unchecked by default; can be changed by the user)
- Default: Y

**Note:**

- A checked **Prompt for more pages** checkbox displays the PaperCut MF Scan Complete (with the two buttons - **Add another page, Send**) screen, to provide users with the option of adding more pages to the scan job.
- An unchecked **Prompt for more pages** checkbox causes the PaperCut MF Scan Complete (with the two buttons - **Add another page, Send**) screen to not be displayed; the process of sending the completed scan job to the user (scan transfer) is automatically initiated; only the PaperCut MF Scan Complete (with scan completed or failed status) screen is displayed. As a result, users are

---

not provided with the option of adding more pages to the scan job.

## "Swipe card" authentication method

### `ext-device.hp-oxpd.register.card-reader`

Customize whether or not PaperCut MF is allowed to automatically register and establish an exclusive lock on card readers that are detected on the device.

This is a device-specific config key.

- Values: Y, N
- Default: Y

#### **Note:**

- Setting this to Y – allows only PaperCut MF to exclusively use card readers, preventing third-party applications from using them. This is recommended only if the **Swipe card** authentication method is selected.
- Setting this to N – allows third-party applications to use card readers. This is recommended if card readers are not used by PaperCut MF for swipe card authentication.

---

### `ext-device.hp-oxpd.additional-card-readers.vid-pid.hex`

Specify the card readers that are supported by PaperCut MF on HP FutureSmart 4 devices, in addition to the list of already supported card readers.

This is a device-specific config key.

- Values: any one or a comma-separated list of `0xVID:0xPID` of card readers (hexadecimal web/HTML notation). For example, for the *Bio-Buddy Converter*, specify `0x2f9f:0x0110`.

**Note:** For more information, see [5.4.1 Supported card readers](#).

---

### `ext-device.card-self-association.use-secondary-card-number`

Customize the use of the primary or the secondary card number slot to save card identifiers during card self-association.

This is a global and device-specific config key.

Device-specific:

---

- Values: Y, N, GLOBAL (inherited from global settings)
- Default: GLOBAL (inherited from global settings)

Global:

- Values: N (Primary), Y (Secondary)
- Default: N

**Note:** This is applicable only if the **Swipe card - Enable self-association with existing user accounts** authentication method is selected. For more information, see [5.3 Authentication methods](#).

---

**ext-device.self-association-allowed-card-regex**

Customize the regular expression filter to be used to validate card identifiers during card self-association.

This is a device-specific config key.

- Values: Any valid regular expression, DEFAULT
- Default: DEFAULT

**Note:** This is applicable only if the **Swipe card - Enable self-association with existing user accounts** authentication method is selected. For more information, see [5.3 Authentication methods](#) and [5.4.3 Methods of handling card](#).

---

**ext-device.card-no-regex**

Customize the regular expression filter to be used to extract card identifiers for authentication.

This is a global and device-specific config key.

Device-specific:

- Values: Any valid regular expression, GLOBAL (inherited from global settings)
- Default: GLOBAL (inherited from global settings)

Global:

- Values: Any valid regular expression

**Note:** This is applicable only if the **Swipe card** authentication method is selected. For more information, see [5.3 Authentication methods](#) and [5.4.3 Methods of handling card](#).

---

---

<b>ext-device.card-no-converter</b>	<p>Customize the converters (standard format converters, custom JavaScript converters, or both) to be used to modify card identifiers for authentication</p> <p>This is a global and device-specific config key.</p> <p>Device-specific:</p> <ul style="list-style-type: none"><li>• Values: Any valid converter (standard format converters, custom JavaScript converters, or both), GLOBAL (inherited from global settings)</li><li>• Default: GLOBAL (inherited from global settings)</li></ul> <p>Global:</p> <ul style="list-style-type: none"><li>• Values: Any valid converter (standard format converters, custom JavaScript converters, or both)</li></ul> <p><b>Note:</b> This is applicable only if the <b>Swipe card</b> authentication method is selected. For more information, see <a href="#">5.3 Authentication methods</a> and <a href="#">5.4.3 Methods of handling card</a>.</p>
-------------------------------------	--

## Job Limits, Zero Stop

---

<b>ext-device.hp-oxpd.limit-reference.duplex</b>	<p>Customize the duplex or simplex attribute of the reference page that is used to determine whether or not a user has sufficient balance to proceed with copying. Based on this value, the corresponding cost of a simplex or duplex copy job is the reference for the minimum balance required for copying. This is then compared to the user's current balance to determine whether or not a user has sufficient balance to proceed with copying.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none"><li>• Values: N (simplex), Y (duplex)</li><li>• Default: N</li></ul> <p><b>Note:</b> This is applicable only to copying for restricted users. For more information, see <a href="#">5.8.1 Job Limits and Zero Stop</a>.</p>
<b>ext-device.hp-oxpd.limit-reference.grayscale</b>	<p>Customize the grayscale or color attribute of the reference page that is used to determine whether or not a user has sufficient balance to proceed with copying. Based on this value, the corresponding cost of a grayscale or color copy job is the reference for the minimum</p>

---

---

balance required for copying. This is then compared to the user's current balance to determine whether or not a user has sufficient balance to proceed with copying.

This is a device-specific config key.

- Values: Y (grayscale), N (color)
- Default: Y

**Note:** This is applicable only to copying for restricted users. For more information, see [5.8.1 Job Limits and Zero Stop](#).

---

**ext-device.hp-oxpd.limit-reference.paper-size**

Customize the paper size of the reference page that is used to determine whether or not a user has sufficient balance to proceed with copying. Based on this value, the corresponding cost of a copy job of the set paper size is the reference for the minimum balance required for copying. This is then compared to the user's current balance to determine whether or not a user has sufficient balance to proceed with copying.

This is a device-specific config key.

- Values: Any valid paper size, DEFAULT
- Default: DEFAULT (North America: Letter; worldwide: A4)

**Note:** This is applicable only to copying for restricted users. For more information, see [5.8.1 Job Limits and Zero Stop](#).

---

**ext-device.hp-oxpd.restricted.multiple-txns**

Customize whether restricted users are permitted or not permitted to perform multiple transactions simultaneously on the device. For example, perform a copy job while another print job is in progress.

This is a device-specific config key.

- Values: N (multiple transactions not permitted), Y (multiple transactions permitted)
- Default: N

**Note:** This is applicable only to restricted users. It is recommended that users are not permitted to perform multiple transactions at a time, to ensure they do not get a negative balance, below the zero limit. For more information, see [5.8.1 Job Limits and Zero Stop](#).

---

## Network resilience, security, debug logs, uninstallation

### **system.network-address**

Specify the network IP address or DNS name of the PaperCut MF Application Server that the device uses to make inbound connections.

This is a global config key.

- Values: Network IP address or DNS name of the PaperCut MF Application Server used by the device for inbound connections

**Note:** For more information, see [5.1.1 Inbound connections to PaperCut MF Application Server](#).

### **ext-device.hp-oxpd.use-ssl**

Toggle the use of the encrypted, secure HTTPS (SSL/TLS) protocol for communication between PaperCut MF and the device.

This is a device-specific config key.

- Values: N (TCP/HTTP), Y (SSL/TLS/HTTPS)
- Default: N (TCP/HTTP)

**Note:** Ensure to set the config key **ext-device.hp-oxpd.port-num** accordingly.

For more information, see [5.2.1 HTTPS Security \(recommended\)](#).

### **ext-device.hp-oxpd.port-num**

Customize the port of the device to be used for communication between PaperCut MF and the device.

This is a device-specific config key.

- Values: 80 (TCP/HTTP), 443 (SSL/TLS/HTTPS), any other valid port number based on your networking/firewall configuration
- Default: 80 (TCP/HTTP)

**Note:** Ensure to set the config key **ext-device.hp-oxpd.use-ssl** accordingly.

For more information, see [5.2.1 HTTPS Security \(recommended\)](#).

### **ext-device.hp-oxpd.period.ping**

Customize the interval of time (seconds) between each attempt made by PaperCut MF to connect to the device.



---

This is a device-specific config key.

- Values: 1-3600 (seconds)
- Default: 300 (seconds)

---

**ext-device.hp-oxpd.period.error**

Customize the interval of time (seconds) between each attempt made by PaperCut MF to connect to the device, after encountering an error when installing PaperCut MF on the device (i.e. device registration and integration).

This is a device-specific config key.

- Values: 1-3600 (seconds)
- Default: 60 (seconds)

---

**ext-device.hp-oxpd.device-setup-complete.delay-secs**

Customize the interval of ramp-up time (seconds) following device registration after which the device can be used.

This is a device-specific config key.

- Values: 0-20 (seconds)
- Default: 5 (seconds)

**Note:** Use this only if there is an open support ticket with PaperCut Support.

## Timeouts

---

**ext-device.inactivity-timeout-secs**

**PaperCut MF timeout:** Customize the interval of time (seconds) after which a logged-in 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 comes into effect only if it is lower than the value of the device's timeout. However, if it is higher, then it is overridden by the lower value of device's timeout. For more information, see [5.12 Timeouts](#).

---

**ext-device.hp-oxpd.timeout.scan-prompt-send.secs**

**PaperCut MF scan complete timeout 1:** Customize the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Complete (with the two buttons - **Add another page**, **Send**) screen is automatically taken to the PaperCut MF

---

Scan Complete (with scan completed or failed status). The process of sending the completed scan job to the user (scan transfer) is also automatically initiated, and the user is logged out.

This is a device-specific config key.

- Values: Any positive integer, DEFAULT
- Default: DEFAULT (30 seconds)

**Note:** This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout. For more information, see [5.12 Timeouts](#).

---

**ext-device.hp-oxpd.timeout.complete-scan-job.secs**

**PaperCut MF scan complete timeout 2:** Customize the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Completes screen (with scan completed or failed status), is automatically logged out.

This is a device-specific config key.

- Values: Any positive integer, DEFAULT
- Default: DEFAULT (5 seconds)

**Note:** This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout. For more information, see [5.12 Timeouts](#).

---

Description of available config keys

## 6 Known Limitations

### 6.1 Zero Stop for USB printing is unavailable

Although printing from a USB or storage device is tracked, it is excluded from the Zero Stop functionality. As a result, a user can get a negative balance below the zero limit if printing from a USB or storage device.

### 6.2 The application of Zero Stop during copying or faxing is delayed

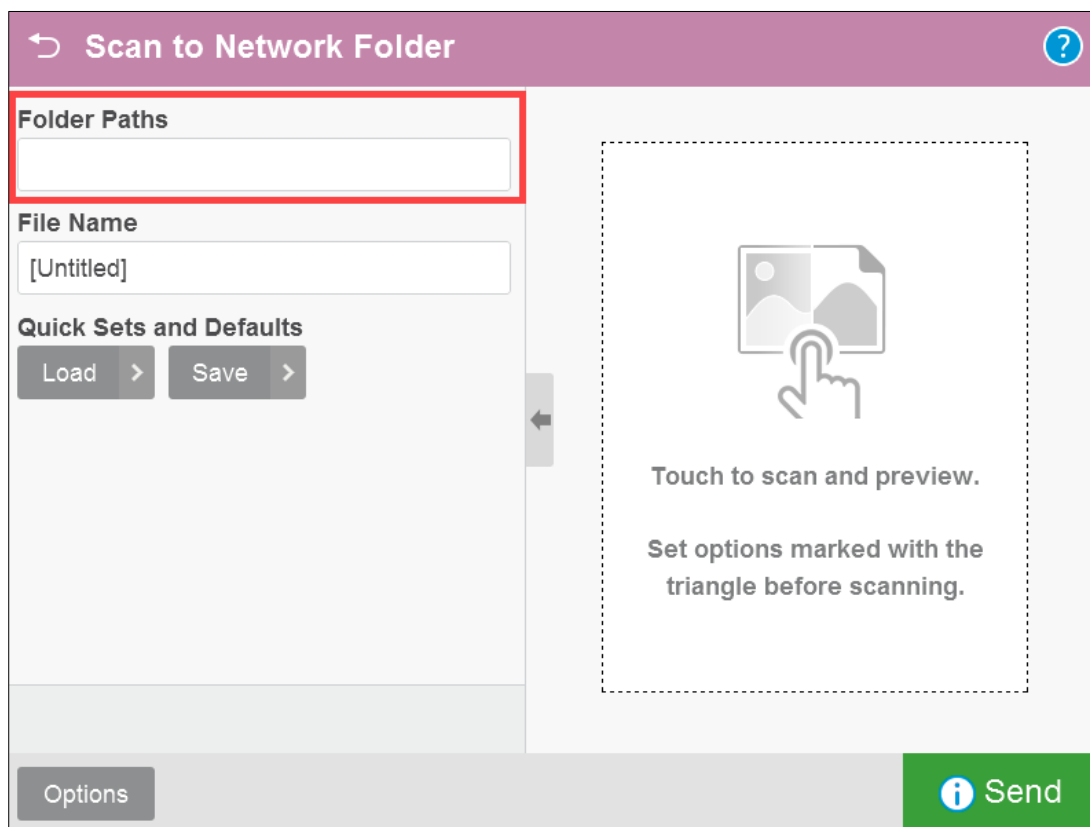
The application of Zero Stop during copying or faxing is delayed and does not stop as soon as it is detected. It is applied after a delay of 8 copied or faxed sheets of paper from when it is detected. As a result, a user can get a negative balance below the zero limit for a maximum of the cost of 8 copied or faxed sheets of paper. The 8 copied or faxed sheets of paper could be 8 simplex or 16 duplex copied or faxed pages.

### 6.3 The application of Zero Stop during simplex scanning is delayed

The application of Zero Stop during simplex scanning is delayed and does not stop as soon as it is detected. It is applied after a delay of 1simplex scanned page from when it is detected. As a result, a user can get a negative balance below the zero limit for a maximum of the cost of 1 simplex scanned page.

### 6.4 The configured user home directory network path is not auto-populated on the device's Scan to Network Folder

While creating and configuring users in PaperCut MF, the user home directory network path is usually configured for all users (**Users > User List > User Details > Home directory**). However, this path is *NOT* auto-populated on the **Scan to Network Folder** screen's **Folder Path** on the device:



As a result, to enable users to use **Scan to Network Folder** on the device, you must configure it on the device's web interface. For more information, see [5.7.3 Device's "Scan to Network Folder"](#).

### 6.5 Some paper sizes are unsupported

Charges for some unsupported paper sizes cannot be configured on the device's **Device Details > Charging** page (they do not appear as an option in the **Add Size** field). As a result, the charge applied if printing, copying, faxing, scanning or UBS printing using any of these paper sizes, is the default charge that is set on the **Device Details > Charging** page.

The list of unsupported paper sizes includes:

- Envelope\_A2\_4point375x5point75in
- Envelope\_Catalog1\_6x9in

- Envelope\_Comm6point75\_3point625x6point5in
- Envelope\_Monarch\_3point875x7point5in
- Envelope\_Windsor\_3point875x8point875in
- Invoice\_5point5x8point5in
- JBusinessCard\_55x91mm
- JDoublePostcard\_148x200mm
- JDoublePostcard\_Rotated\_148x200mm
- JIS\_Chou3\_120x235mm
- JIS\_Chou4\_90x205mm
- JIS\_Exec\_216x330mm
- JIS\_Kaku2\_240x332mm
- JPostcard\_100x148mm
- LongScan\_8point5x34in
- Mutsugiri\_203x254mm
- ISO\_A\_8\_52\_X\_74\_MM
- ISO\_A\_9\_37\_X\_52\_MM
- ISO\_A\_10\_26\_X\_37\_MM
- ISO\_B\_8\_62\_X\_88\_MM
- ISO\_B\_9\_44\_X\_62\_MM
- ISO\_B\_10\_31\_X\_44\_MM
- ISO\_C\_0\_917\_X\_1297\_MM
- ISO\_C\_1\_648\_X\_917\_MM
- ISO\_C\_2\_458\_X\_648\_MM
- ISO\_C\_7\_81\_X\_114\_MM
- ISO\_C\_8\_57\_X\_81\_MM
- ISO\_C\_9\_40\_X\_57\_MM
- ISO\_C\_10\_28\_X\_40\_MM
- JIS\_B\_0\_1030\_X\_1456\_MM
- JIS\_B\_6\_128\_X\_182\_MM
- JIS\_B\_7\_91\_X\_128\_MM
- JIS\_B\_8\_64\_X\_91\_MM
- JIS\_B\_9\_45\_X\_64\_MM
- JIS\_B\_10\_32\_X\_45\_MM
- DIN\_2\_A\_0\_1189\_X\_1682\_MM
- DIN\_4\_A\_0\_1682\_X\_2378\_MM
- ENVELOPE\_DL\_110\_X\_220\_MM
- GENERAL\_3\_POINT\_5\_X\_5\_IN
- GENERAL\_3\_X\_5\_IN
- GENERAL\_4\_X\_6\_IN
- GENERAL\_4\_X\_8\_IN
- GENERAL\_4\_X\_12\_IN
- GENERAL\_5\_X\_7\_IN
- GENERAL\_5\_X\_8\_IN

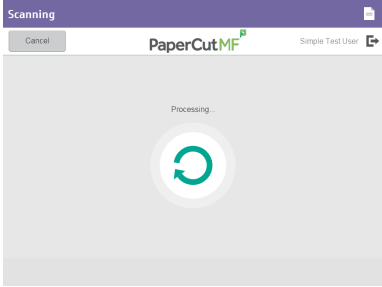
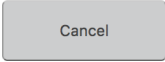

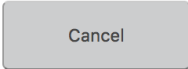
- GENERAL\_6\_X\_8\_IN
- GENERAL\_7\_X\_9\_IN
- GENERAL\_10\_X\_13\_IN
- GENERAL\_10\_X\_15\_IN
- GENERAL\_11\_X\_12\_IN
- GENERAL\_11\_X\_14\_IN
- GENERAL\_11\_X\_19\_IN
- GENERAL\_12\_X\_12\_IN
- GENERAL\_12\_X\_14\_IN
- GENERAL\_12\_X\_19\_IN

## 6.6 Scanning continues even if the feeder or glass is empty

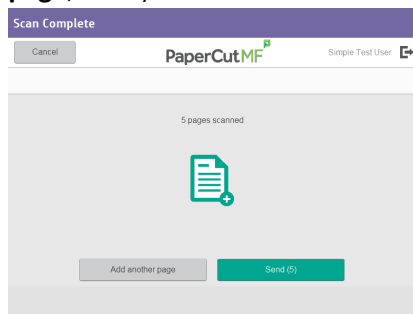
If using Integrated Scanning, the pages to be scanned must be placed on the document feeder or the glass before starting the scan. If the document feeder or the glass is empty, the device does not prompt users with a relevant message. Scanning continues, producing a blank scanned page that is tracked and charged.

## 6.7 The "Cancel" and "Logout" buttons behave inconsistently on the PaperCut MF Integrated Scanning screens

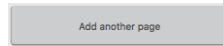
The "Cancel" and "Logout" buttons behave inconsistently on the PaperCut MF Integrated Scanning screens:

PaperCut MF screen	"Cancel" or "Logout"	Impact
<p>The PaperCut MF Scanning screen (with a processing spinning wheel)</p> 		<ul style="list-style-type: none"> <li>• The scan job is aborted</li> <li>• The scan job not sent to the user</li> <li>• The scan job is tracked</li> <li>• The user is charged</li> </ul>
		<ul style="list-style-type: none"> <li>• The user is logged out</li> <li>• The scan job is not aborted</li> <li>• The scan job is sent to the user</li> <li>• The scan job is tracked</li> <li>• The user is charged</li> </ul>
<p>The PaperCut MF Scan Complete screen (with the two buttons - <b>Add another</b></p>		<ul style="list-style-type: none"> <li>• The scan job is not aborted</li> <li>• The scan job is not sent to the user</li> <li>• The scan job is tracked</li> <li>• The user is charged</li> </ul>

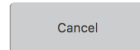
page, Send)



- The user is logged out
- The scan job is not aborted
- The scan job is sent to the user
- The scan job is tracked
- The user is charged



and

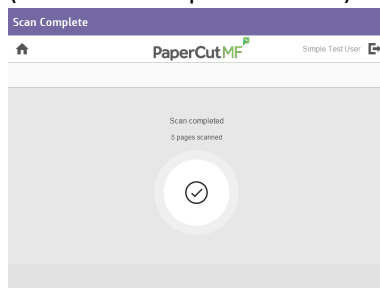


or



- Only the last scan job is aborted; it is not sent to the user; it is not tracked; the user is not charged.
- However, all the other scan jobs before the last scan job are not aborted; the scan jobs are not sent to the user; but they are tracked, and the user is charged.

The PaperCut MF Scan Complete screen (with scan completed status)

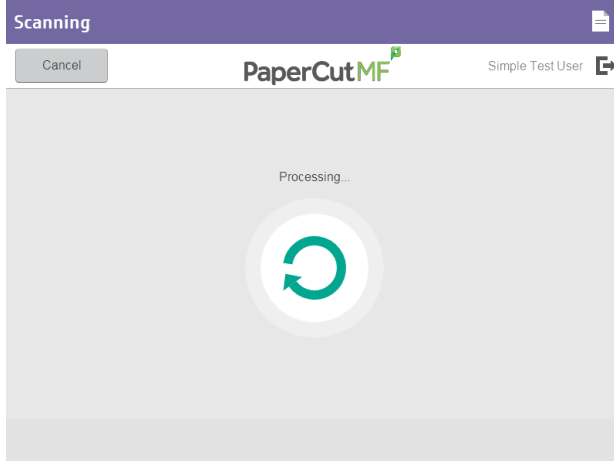


- The user is logged out
- The scan job is not aborted
- The scan job is sent to the user
- The scan job is tracked
- The user is charged

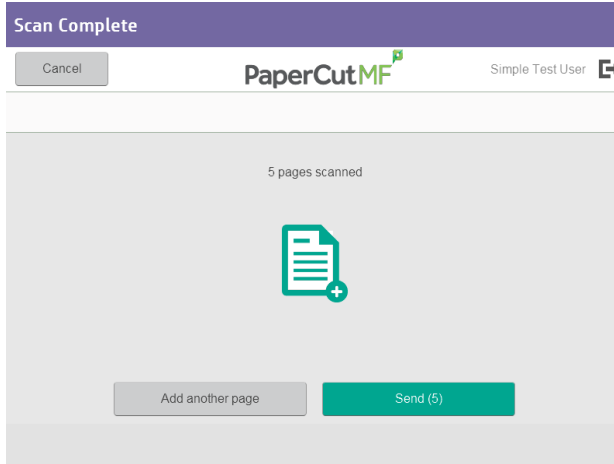
## 6.8 Impact of environmental factors on Integrated Scanning

If using Integrated Scanning, then the occurrence of some environmental changes (such as, Application Server outage, device is disconnected and restarted, network outage) when the user is on any of the following screens, causes the scan job to be tracked and the user is charged, although the scan job is not sent to the user:

- The PaperCut MF Scanning screen (with a processing spinning wheel), or



- The PaperCut MF Scan Complete screen (with the two buttons - **Add another page**, **Send**)



## 6.9 Attributes of scan job logs are unavailable

The PaperCut MF Admin web interface (Logs > Job Log) does not display the Attributes (page size, duplex or simplex, and color or grayscale) of scan jobs. The column is either blank or just displays invoice comments (if any).

DATE ▼	USER	CHARGED TO	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Apr 26, 2018 10:17:30 AM	simpletestuser	simpletestuser	1	\$0.11	[scanning] - scan ... -5c7ba703c959-01.pdf	 Comment	← Scanned refund edit

# 7 Uninstall *PaperCut MF - HP OXP*

## 7.1 Temporarily disable *PaperCut MF - HP OXP*

To temporarily disable *PaperCut MF - HP OXP*:

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

- In the **Configuration** area's **Enable/Disable**, select a **Disable** option:

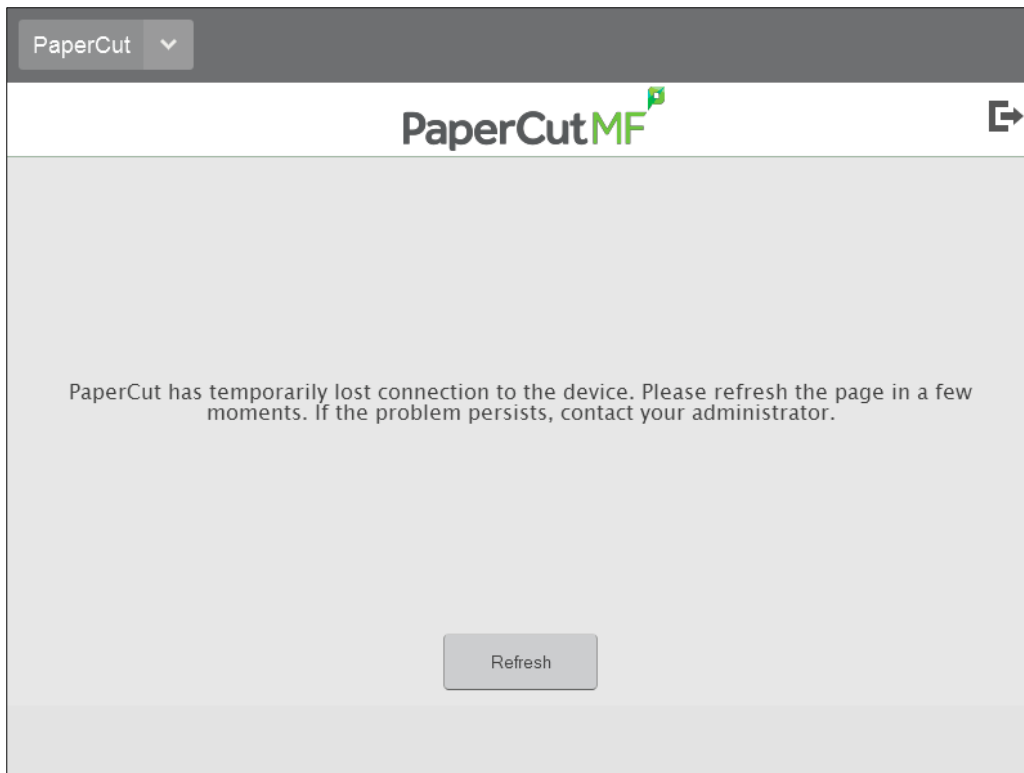
The screenshot shows the 'Configuration' page with tabs for Summary, Charging, Filters & Restrictions, Job Log, Statistics, and Advanced Config. The 'Configuration' section includes a description: 'Simple configuration options. Advanced configuration options are available below and on the other tabs.' Below this is the 'External Device Settings' section with the text: 'Allows for the configuration of the external device. For example connection settings like IP addresses and ports.' On the right side, there are fields for 'Physical identifier' (net://hp-fs4-sim) and 'Location/Department'. The 'Enable/Disable' section shows a dropdown menu with the following options: 'Enabled' (checked), 'Disable for next 10 minutes', 'Disable for next 30 minutes', 'Disable for next hour', 'Disable until tomorrow', 'Disable for 1 week', 'Disable for 2 weeks', 'Disable for 1 month', and 'Disable indefinitely'.

- Verify that *PaperCut MF - HP OXP* is disabled:

The screenshot shows the 'Configuration' page with the same layout as the previous image. The 'Enable/Disable' section now shows a lock icon followed by the text: 'Disabled until Oct 6, 2017 11:28:58 AM (Enable)'. The other fields and sections remain the same.

- Verify that *PaperCut MF - HP OXP* is not available on the device to users:

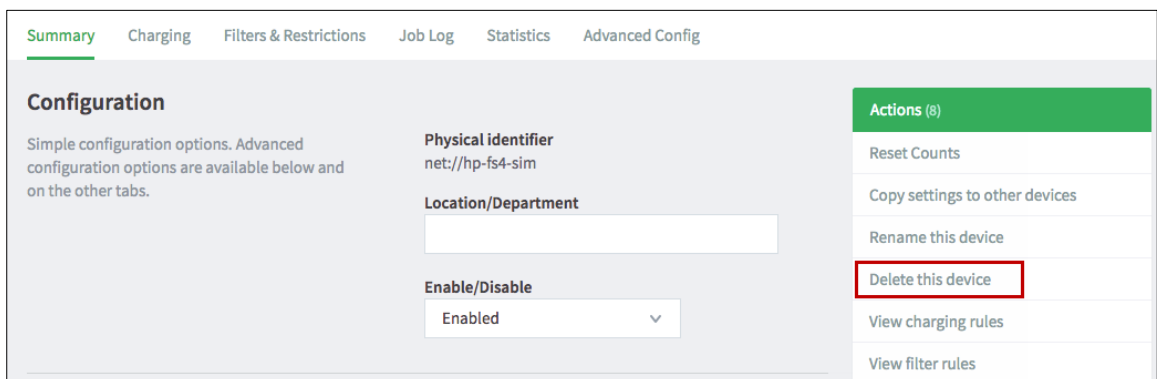




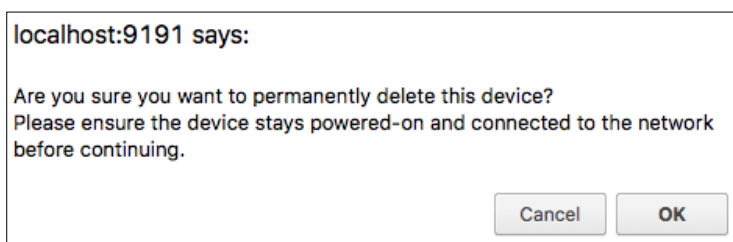
## 7.2 Permanently uninstall *PaperCut MF - HP OXP*

To permanently uninstall *PaperCut MF - HP OXP*:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. Click **Actions > Delete this device**:

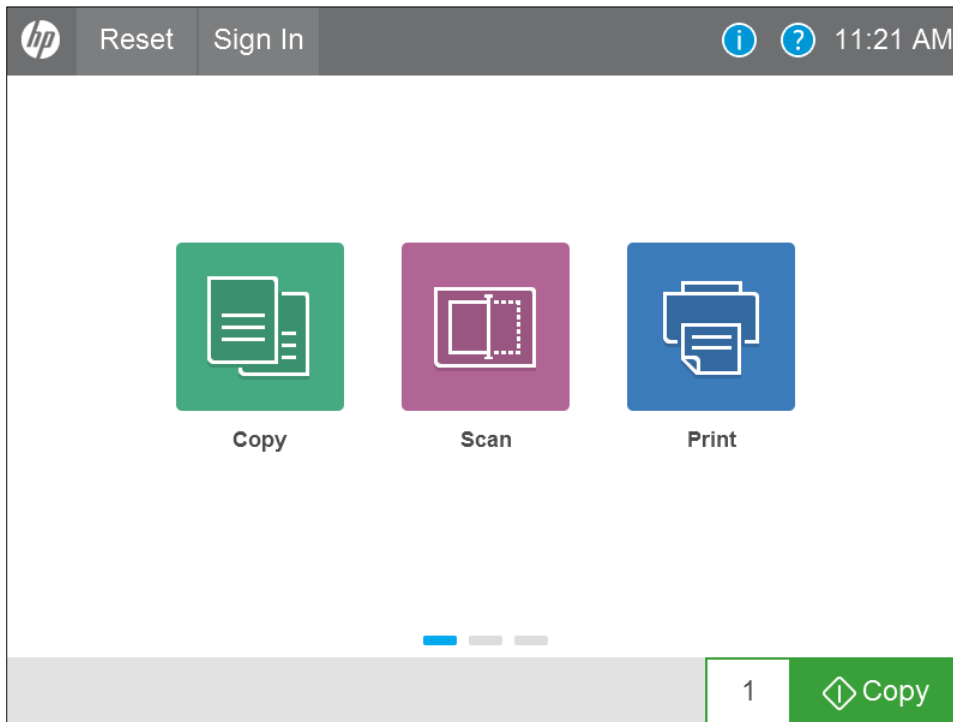


5. Click **Ok**:



6. Click **Devices** and verify that the device is no longer listed (*PaperCut MF - HP OXP* is permanently uninstalled).

7. Verify that *PaperCut MF - HP OXP* is not available on the device to users:



## 8 FAQ & Troubleshooting

### 8.1 IP addresses of the PaperCut MF Application Server

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

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

### 8.2 Device Status "Started (with errors)"

After attempting to create the device (PaperCut MF installation or device registration and integration), if the **Device Status** displays **Started (with errors)**, it implies that PaperCut MF installation is unsuccessful because there are errors in the **Create Device** fields (**Type**, **Device name**, **Hostname / IP**, **Device's administrator** credentials) or errors on the device or both.



To resolve this:

1. Address any device-specific errors outlined on the device.
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Devices**.

4. Click the **Device Name** of the device displaying the error status in the **Status** column.
5. Resolve the error based on the cause and resolution as outlined in the **Device Status**.
6. Click **Apply**.

### 8.3 Swipe card authentication anomalies

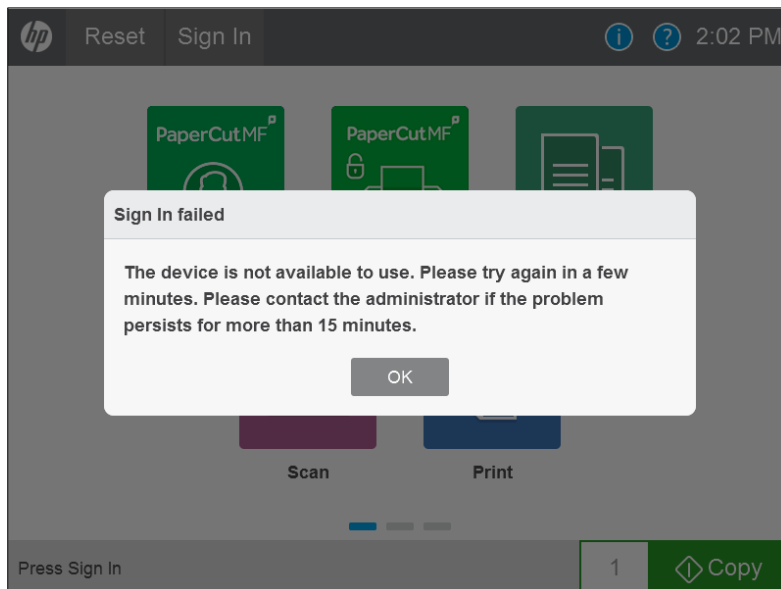
After PaperCut MF is successfully installed on the device, if swipe card authentication causes some problems during login or during card self-association, it implies that the card reader configuration on the PaperCut MF Admin web interface is incorrect.

To resolve this:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In the **External Device Settings** area's **Swipe card > Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)** ensure that if any one of the following card types is selected, then its conflicting other is not also selected as another card type:
  - **Either** HID Prox **or** HID Prox UID
  - **Either** MiFare CSN (Philips, NXP) **or** MiFare Ultralight CSN (Philips, NXP)
  - **Either** MiFare CSN (Philips, NXP) **or** iClass CSN, ISO1443A CSN, ISO15693A (RDR-758x Compatible)

### 8.4 "Device is not available to use" error

After PaperCut MF is successfully installed on the device, if the device displays the following error when users attempt to log in, it implies that incorrect modifications have been made to the device's settings on the **Devices > External Device List > Device Details** page:



To resolve this:

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

3. Click the **Device Name** of the device displaying the error status in the **Status** column.
4. Resolve the error based on the cause and resolution as outlined in the **Device Status** area.
5. Click **Apply**.

## 8.5 Device Status "Started (with errors) – Certificate error"

After attempting to enable HTTPS, if the **Device Status** displays **Started (with errors) – Certificate error**, it implies that the limited number of certificates allowed on the device has been exceeded:

**Device Status**

Started (with errors) – Certificate error.

Error: Device's certificate store has reached its maximum size. Delete unused certificates.

Last updated Mar 5, 2018 2:42:57 PM Refresh

To resolve this:

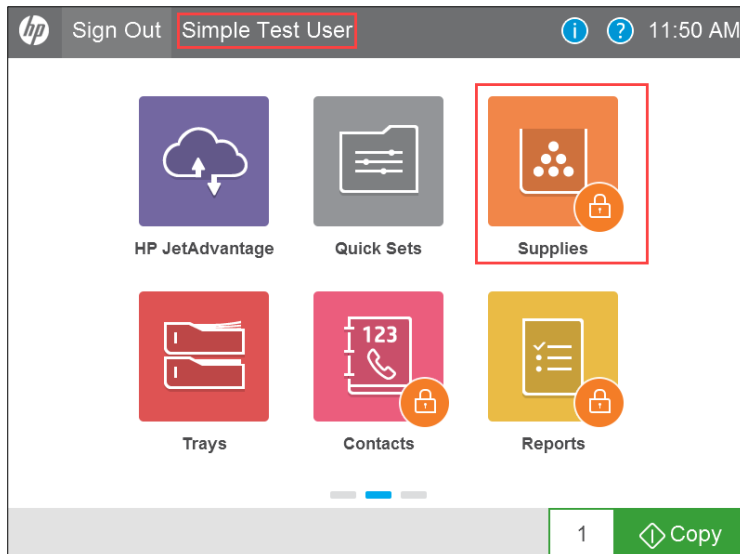
1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Certificate Management**:

Issued To	Issued By	Expiration Date	Certificate
<input checked="" type="radio"/> hp-e77830.papercutssoftware.com	hp-e77830.papercutssoftware.com	13 Aug, 2022 04:18:52	Self-Sig
<input type="radio"/> Baltimore CyberTrust Root	Baltimore CyberTrust Root	12 May, 2025 06:59:00	Root CA
<input type="radio"/> DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	9 Nov, 2031 05:00:00	Root CA
<input type="radio"/> Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	21 Jan, 2018 23:41:51	Root CA
<input type="radio"/> GlobalSign Root CA	GlobalSign Root CA	27 Jan, 2028 17:00:00	Root CA
<input type="radio"/> VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	16 Jul, 2036 06:59:59	Root CA
<input type="radio"/> hp-e77830.papercutssoftware.com	hp-e77830.papercutssoftware.com	13 Aug, 2022 04:18:52	Self-Sig
<input type="radio"/> hello	hello	5 Oct, 2037 01:22:55	Root CA

3. Delete any unused certificates.
4. Log in to the PaperCut MF Admin web interface.
5. Navigate to **Devices**.
6. Select the device.
7. Click **Apply**.

## 8.6 Administrative device functions are unavailable to users

By default, PaperCut MF locks certain administrative device functions (such as, Supplies, Contacts, Reports, Settings, Support Tools, Job Log) on the device, making them available only to administrators. These appear with a lock icon to non-administrative users (such as, the simple test user). Clicking a locked administrative device function, displays an error message.



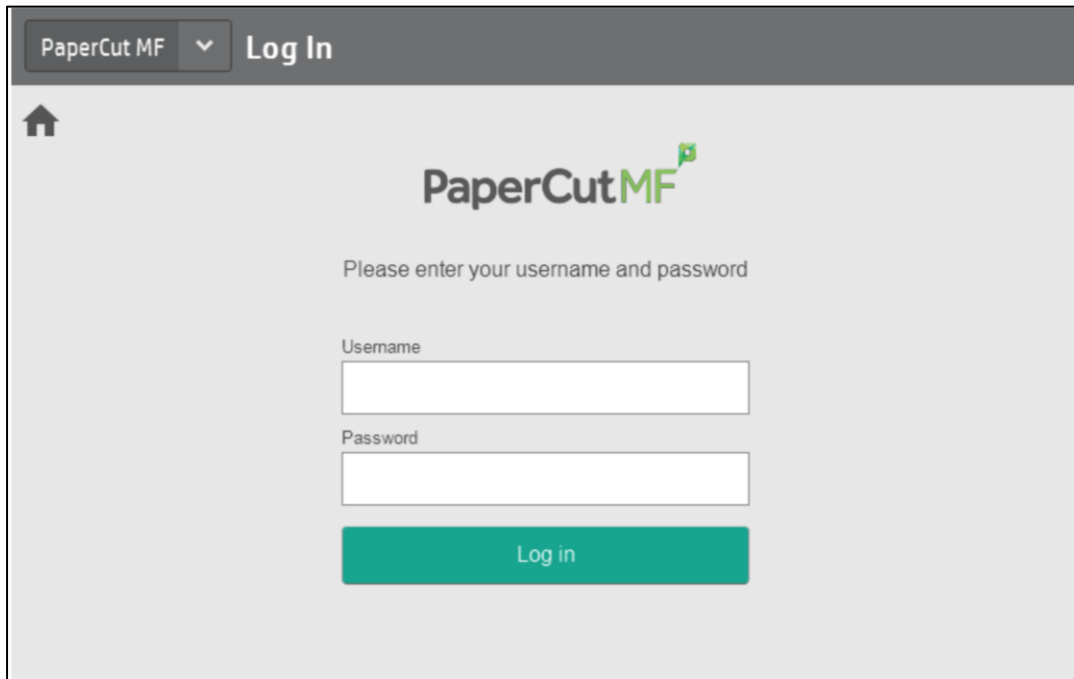
**Note:** For more information about changing these access permissions and restrictions, see [5.5.2.2 Using the device's Access Control to customize access to device functions](#).

## 8.7 Third-party applications are unable to use card readers

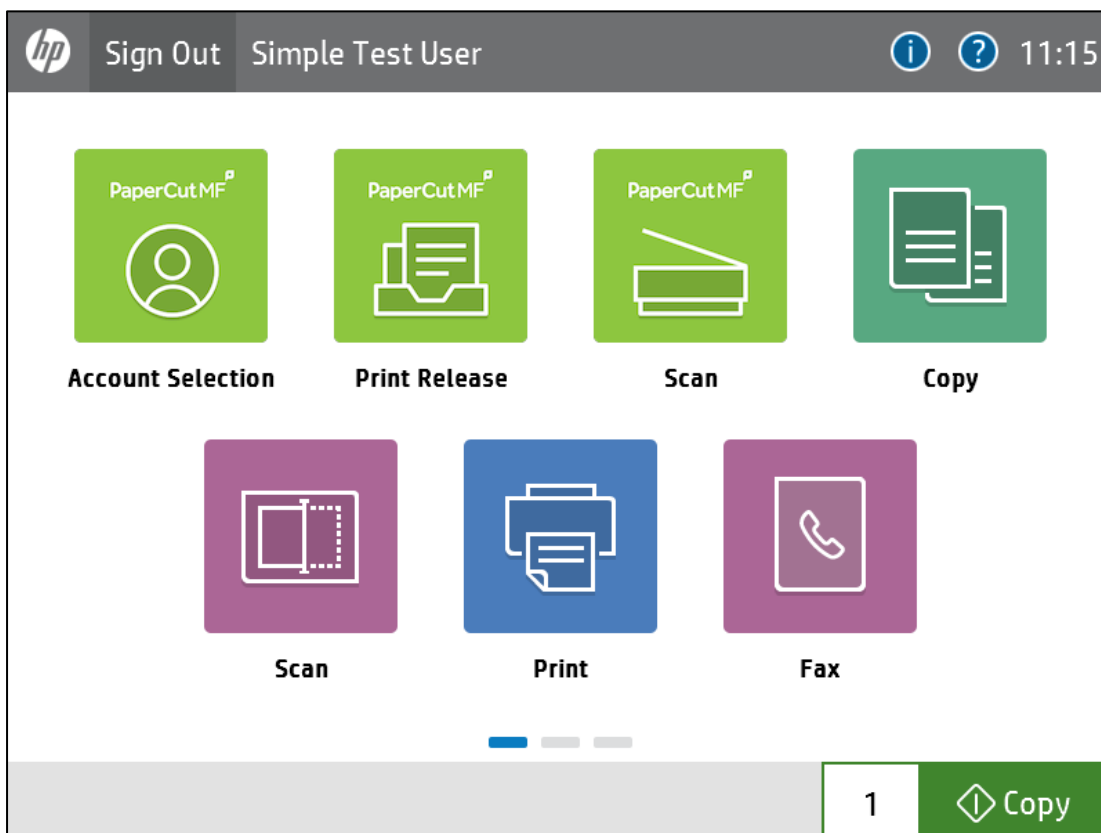
PaperCut MF automatically registers and establishes an exclusive lock on card readers that are detected on the device. As a result, they cannot be used by any other third-party applications. If the **Swipe card** authentication method is not selected (PaperCut MF is not being used for swipe card authentication), but third-party applications require access to card readers, then ensure to set the config key `ext-device.hp-oxpd.register.card-reader` to **Y**. For more information, see [5.13 Config Editor](#).

## 9 Appendix A: Device screens

The PaperCut MF Login screen (default authentication):

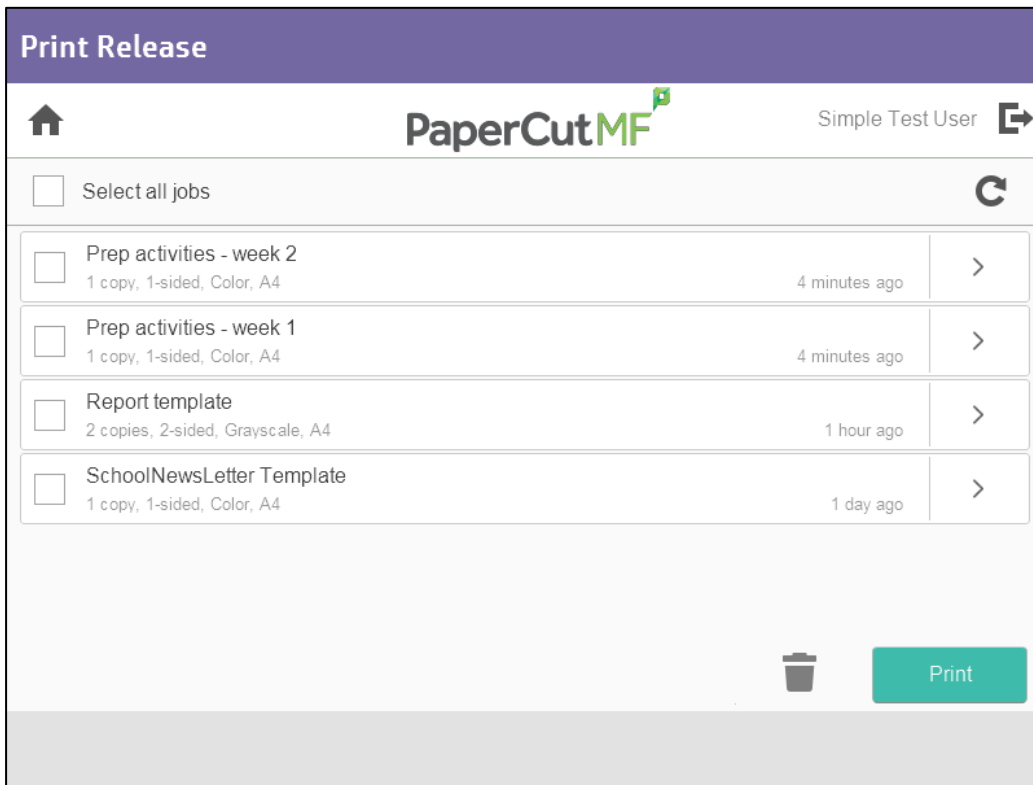


The non-PaperCut MF device screen with **PaperCut MF Integrated Scanning** and **Account Selection** icons:

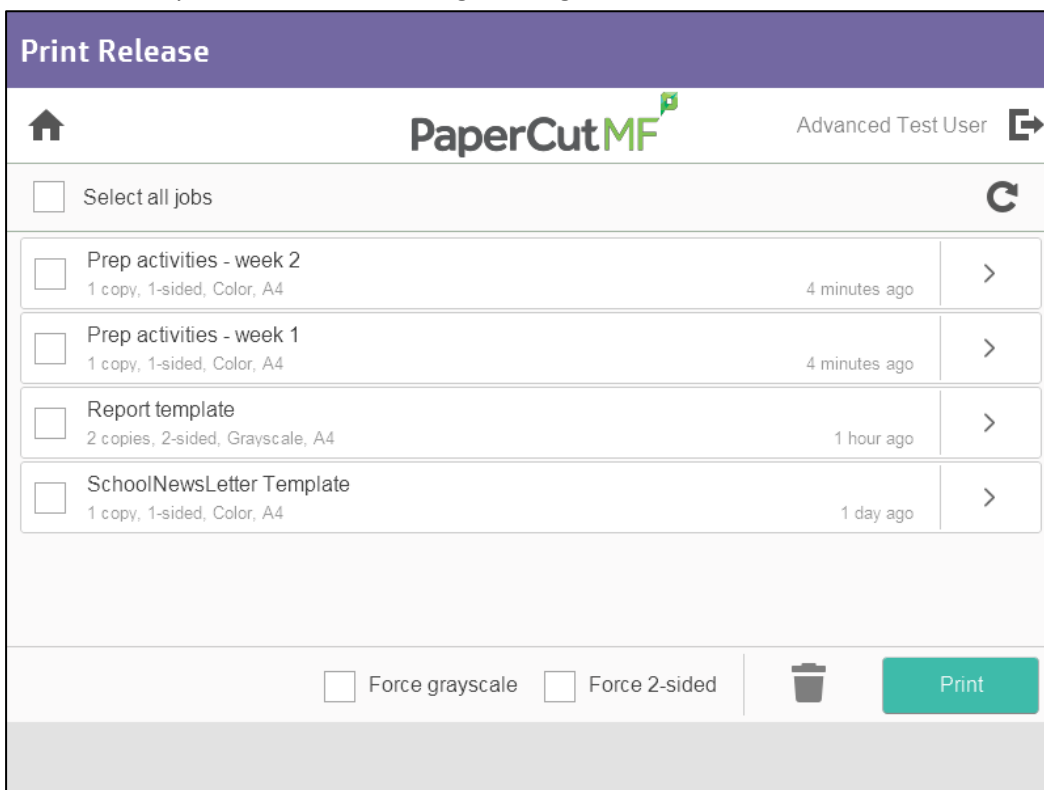


The PaperCut MF Print Release screen with all held print jobs:

- Without the ability to allow users to change settings:



- With the ability to allow users to change settings:



The PaperCut MF Print Settings screen with details of one held print job:

- Without the ability to allow users to change settings:

**Print Settings**

<
PaperCut<sup>MF</sup>
Simple Test User

---

Print Release > Prep activities - week 1

<b>Time</b>	Jun 22, 2018 10:53:57 AM	<b>Copies</b>	1
<b>User</b>	simpletestuser	<b>Duplex mode</b>	1-sided
<b>Pages</b>	3	<b>Color mode</b>	Color
<b>Account</b>	DEFAULT	<b>Page size</b>	A4
<b>Balance</b>	\$100.00	<b>Cost</b>	\$0.51

Print

- With the ability to allow users to change settings:

**Print Settings**

<
PaperCut<sup>MF</sup>
Advanced Test User

---

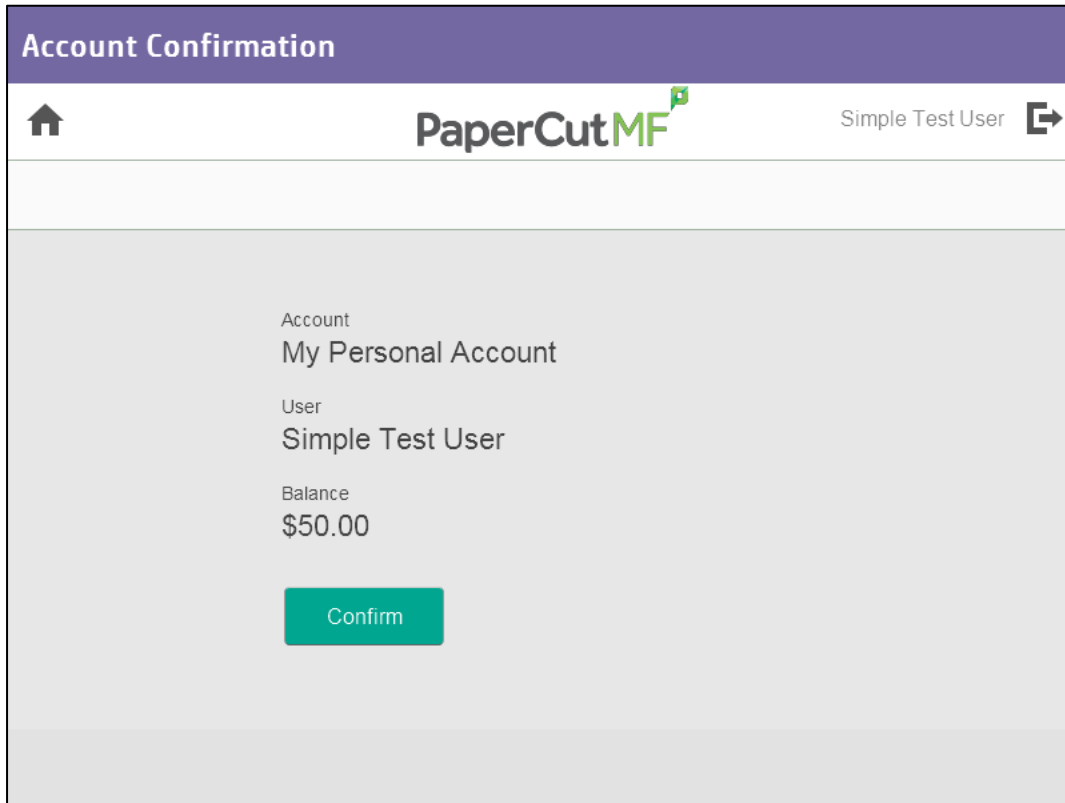
Print Release > Prep activities - week 1

<b>Time</b>	Jun 13, 2018 4:41:03 PM	<b>Copies</b>	<input type="button" value="-"/> <input style="width: 30px; text-align: center;" type="text" value="1"/> <input type="button" value="+"/>
<b>User</b>	advancedtestuser	<b>Duplex mode</b>	<input checked="" type="radio"/> 1-sided <input type="radio"/> 2-sided
<b>Pages</b>	1	<b>Color mode</b>	<input type="radio"/> Color <input checked="" type="radio"/> Grayscale
<b>Account</b>	Test Account	<b>Page size</b>	A4
<b>Balance</b>	\$50.00	<b>Cost</b>	\$2.50 <span style="background-color: #333; color: white; padding: 2px 5px; font-size: 0.8em;">Saved \$0.62</span>

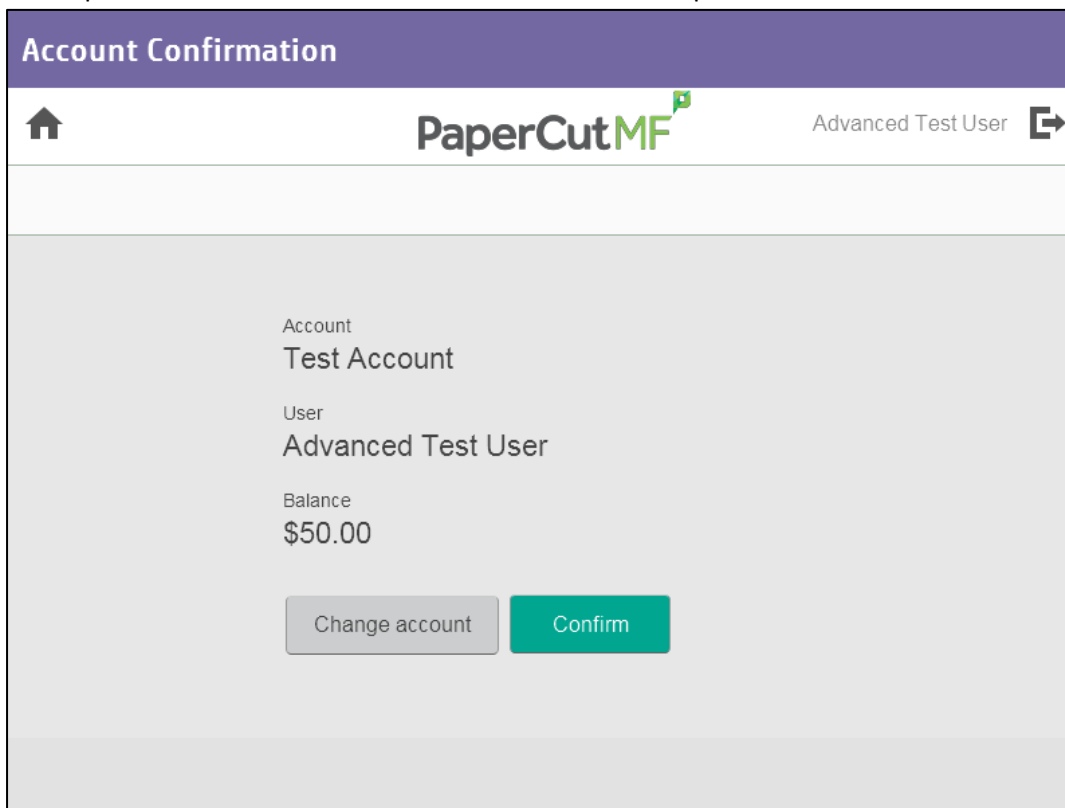
Reset to original
Print



The PaperCut MF Account Confirmation screen without the option of account selection:



The PaperCut MF Account Confirmation screen with the option of account selection:



The PaperCut MF Account Selection screens:

This screenshot shows the 'Account Selection' screen. At the top, there is a purple header with the text 'Account Selection'. Below the header is a white navigation bar containing a home icon, the 'PaperCutMF' logo, and the text 'Advanced Test User' with an external link icon. The main content area features a search input field with the placeholder text 'type account name'. To the right of the input field are two radio buttons: 'By Name' (which is selected) and 'By Code'. A green 'Search' button is positioned to the right of these options. Below the search controls, a list of account names is displayed: 'My Personal Account' and 'Test Account'. The background of the main content area is a light gray gradient.

This screenshot shows the 'Account Selection' screen with the search criteria changed. The header and navigation bar are identical to the first screenshot. In the search input field, the placeholder text is 'type account code'. The 'By Code' radio button is now selected, and the 'By Name' button is unselected. The green button is now labeled 'Select'. The list of account names is empty, and the background remains a light gray gradient.

The screenshot shows the 'Account Selection' interface. At the top, there is a purple header with the title 'Account Selection'. Below the header is a navigation bar containing a home icon, the 'PaperCutMF' logo, and the text 'Advanced Test User' with an external link icon. The main content area features a search input field with the placeholder text 'type account name' and a teal 'Search' button. Below the search field, a list of account names is displayed: 'My Personal Account' and 'Test Account'.

This screenshot shows the 'Account Selection' interface with a different search criteria. The header and navigation bar are identical to the previous screenshot. The search input field now has the placeholder text 'type account code' and a teal 'Select' button. Below the search field, the text 'Or' is centered, followed by a list of account names: 'My Personal Account'.

The PaperCut MF Integrated Scanning screens:

1. The PaperCut MF Scan screens:

### Scan Actions

Home PaperCut<sup>MF</sup> Simple Test User

Account: My Personal Account

- Scan to Email
- Scan to Folder

### Scan Details

Back PaperCut<sup>MF</sup> Simple Test User

Account: My Personal Account Balance: \$99.80

**Scan to Folder**

Path  
usr/test/Scans

Filename  
scan\_fx\_2018-03-02-11-55-19

Color PDF

1-sided

A4 Portrait

300 DPI

Change settings

Prompt for more pages  Start

### Scan Settings

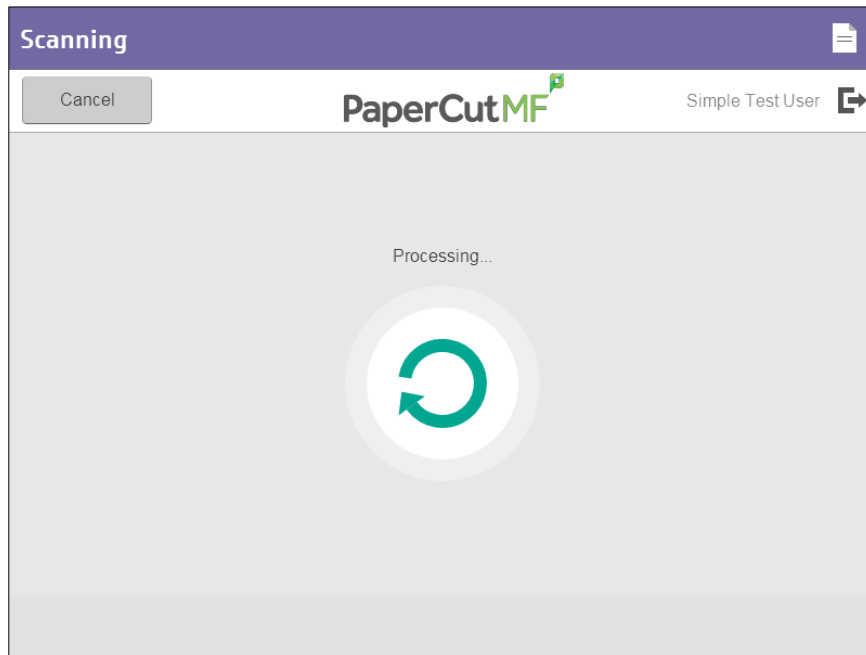
Back PaperCut<sup>MF</sup> Simple Test User

Scan Settings > Scan to Folder

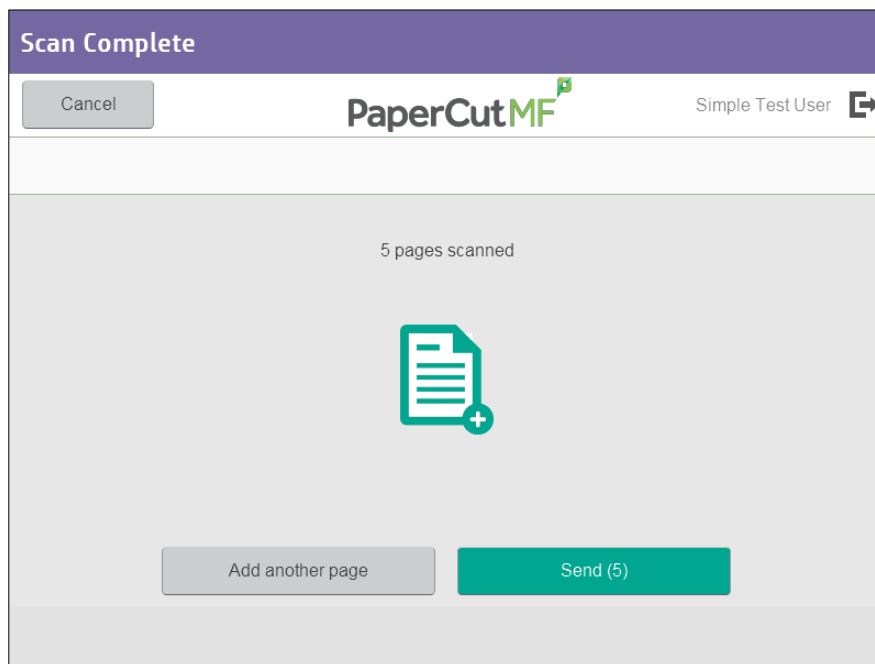
Duplex mode	<input checked="" type="radio"/> 1-sided <input type="radio"/> 2-sided	File type	<input checked="" type="radio"/> PDF <input type="radio"/> JPEG <input type="radio"/> TIFF
Orientation	<input checked="" type="radio"/> Portrait <input type="radio"/> Landscape	DPI	<input type="radio"/> 200 <input checked="" type="radio"/> 300 <input type="radio"/> 400 <input type="radio"/> 600
Paper size	<input checked="" type="radio"/> A4 <input type="radio"/> A5	Color mode	<input checked="" type="radio"/> Color <input type="radio"/> Grayscale <input type="radio"/> B&W

Prompt for more pages  Start

2. The PaperCut MF Scanning (with a processing spinning wheel) screen:



3. The PaperCut MF Scan Complete (with the two buttons - **Add another page, Send**) screen:



4. The PaperCut MF Scan Complete (with scan completed or failed status) screen:

