PaperCut MF - HP FutureSmart Legacy Embedded Manual

Contents

1 Version history

PaperCut MF version or date	Details
18.3.3	6.1 Config Editor
18.2.0	5.4 Shared Account Selection, 6.1 Config Editor
18.1.1	3.2.5 PaperCut Settings

2 Overview

This manual covers PaperCut's embedded software solution, PaperCut MF - HP FutureSmart Legacy, for compatible HP FutureSmart 3 devices. For general PaperCut MF documentation, see the PaperCut MF manual.

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

- Secure access to device functions
- End-user authentication including integration with single sign-on environments
- Monitoring and control of photocopying (quotas, charging, allocation and logging)
- Allocation of copying to accounts/departments/cost centers/projects (shared accounts)
- Ability to locate shared accounts via select-from-list, keyword search or manual code/pin entry
- Release jobs from a hold/release queue (Secure & Find Me Printing)
- Tracking of faxing and scanning

Highlights of the embedded 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 workstation print interface, meaning users only have to learn one system.

2.2 Integration

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

2.3 Rate of development

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

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

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

3 Installation

This section covers the installation of PaperCut MF - HP FutureSmart Legacy for compatible HP FutureSmart 3 devices. The embedded application will allow the control, logging and monitoring of walk-up off-the-glass copier, fax and scanner usage and may serve as a release station for network prints (for information on tracking network printing see the PaperCut user manual).

3.1 Requirements

Ensure that the following points are checked off before getting started:

- The devices on your network are HP FutureSmart 3 devices (HP FutureSmart devices running the HP FutureSmart 3 platform). For more information, see 3.1.1 Determine the HP Platform
- The HP FutureSmart 3 devices on your network are compatible with PaperCut's embedded software solution, PaperCut MF - HP FutureSmart Legacy. Most HP FutureSmart 3 devices are compatible with PaperCut MF - HP FutureSmart Legacy, except:
    - scanner-only devices, and
    - devices with 4-line displays

  For more information, see PaperCut MF for HP.

  For more information on PaperCut's embedded solutions for other devices and platforms, contact your reseller or Authorized Solution Center.
- The devices on your network are directly accessible by the PaperCut MF Application Server (i.e. not via a NAT network).
- The HP devices have an administrator username and password defined for access to their web admin.
- The networking/firewall configuration allows:
    - Inbound connections to the PaperCut MF Application Server from your devices on your configured ports. For example:
        - 9191 (TCP/HTTP)
        - 9192 (TCP/HTTPS)
    - Outbound connections from the PaperCut MF Application Server to your devices on your configured ports. For example:
        - 7627 (TCP/HTTPS)
- The latest version of PaperCut MF is installed and running on your network. For more information, see the PaperCut MF manual.

3.1.1 Determine the HP Platform

To determine the HP platform running on the device:

1. Log into the device's EWS.
2. Navigate to **Information → Configuration Page**

3. Look for the **Firmware Version** label in the **Device Information** section.

On Chai devices, this label is missing (but " **Firmware Datecode** " will be present).

On FutureSmart devices, the value begins with "FutureSmart"

Firmware Version: FutureSmart 2 SP1 (2200643_228337)

Firmware Revision: 2200643_228337

Note: This manual covers PaperCut's embedded software solution, PaperCut MF - HP FutureSmart Legacy, for compatible HP FutureSmart 3 devices.

3.1.2 Uninstall PaperCut MF - HP OXP

This is applicable only if your HP FutureSmart 4 device (i.e. HP FutureSmart device running the HP FutureSmart 4 platform that is compatible with both PaperCut MF - HP FutureSmart Legacy and PaperCut MF - HP OXP) already has PaperCut's embedded software solution PaperCut MF - HP OXP installed. In that case, you must uninstall the existing PaperCut MF - HP OXP before attempting to install PaperCut MF - HP FutureSmart Legacy.

To uninstall PaperCut MF - HP OXP from the device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. Click **Actions > Delete this device**:
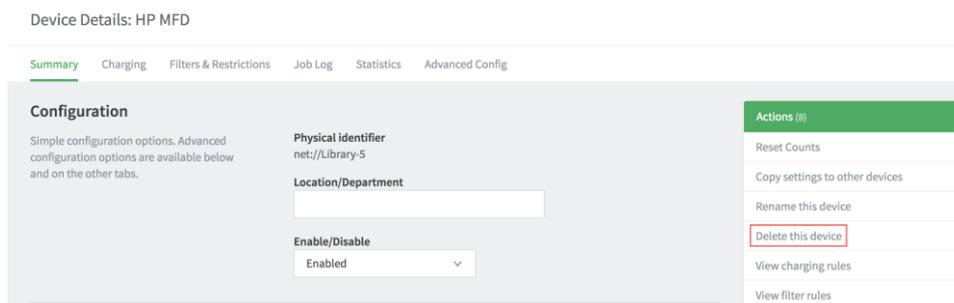
5. Click **Ok:**
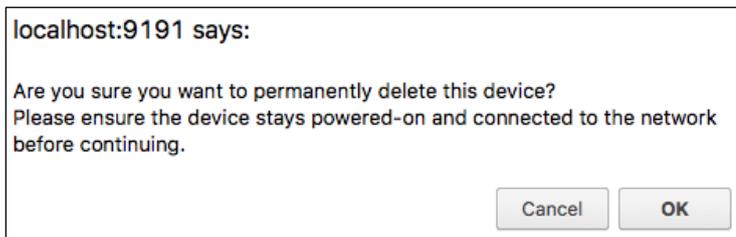
6. Click **Devices** and verify that the device is no longer listed (PaperCut MF - HP OXP is permanently uninstalled).
7. Verify that PaperCut MF - HP OXP is not available on the device to users:

---

hp   Reset   Sign In   ⓘ ❓ 11:21 AM

Copy   Scan   Print

[1 | ◇ Copy]
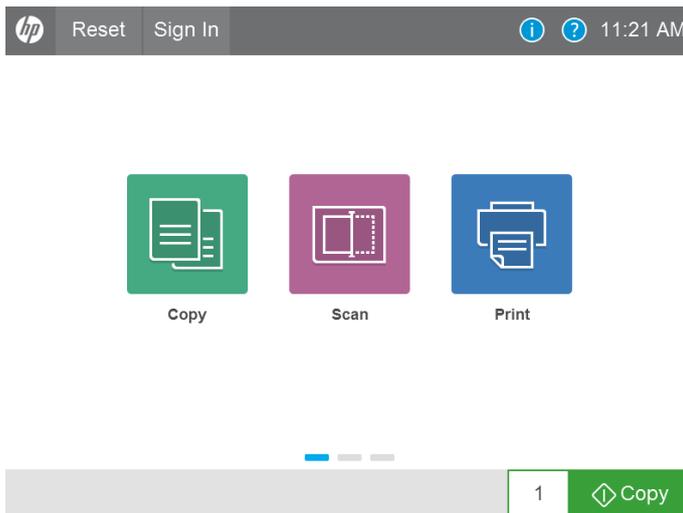
3.2 Setup Procedure

3.2.1 Deploy the PaperCut App Using the Device's Web Admin

1. Using a web browser, navigate to the HP device's web admin, e.g. **http://staff-room-hp/**

2. Click **Sign In** in the top-right corner of the page and sign in using device administrator credentials.

3. Navigate to **General → Solution Installer** .

4. Under Install New Solution select a file to upload and pick `[app-path]/providers/hardware/hp-futuresmart/pc-hp-futuresmart-CE.bdl`
   then click **Install**.

3.2.2 Tell Device Where to Find PaperCut Server

1. After deploying the app, a new menu item **PaperCut Server Configuration** should appear on the **General** tab in the device's web admin. Navigate to this page.

2. Enter the **Server hostname or IP address** of the PaperCut primary server.

3. Enter a unique **Device name** . This will be the name of the device on the **Devices** tab in the PaperCut admin interface. E.g. "`Staff Room MFP`".

4. Click **Configure**.

3.2.3 Configure Device Access Control

These steps are required to enforce color access control, and are recommended even if you do not plan on restricting access to color copying.

1. In the HP device's web admin, navigate to **Security → Access Control** .

2. Click the checkbox below the **Device Guest** column header until all the checkboxes in that column change to locks. This disables all guest functionality by default.

---
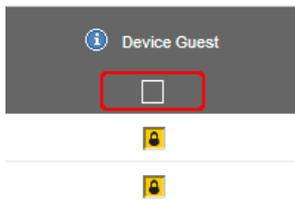
3. In the **Device Guest** column:

    a. **For color devices:** Expand the **Printing** item (click on the **+** icon) and enable

        (change to a green tick) the **Print in color** item. If this option is left as restricted,

        network print jobs will be automatically converted to grayscale.

    b. Enable any functionality that you would like to allow without requiring sign-in (e.g. scanning, if you will not be tracking it).

4. **For color devices:** In the **Device User** column, uncheck (change to an empty box) the option

    Copy application → Make a Color Copy . This is required to allow PaperCut to perform

    color copying access control.

5. Click the **Apply** button at the bottom of the page.

3.2.4 Disable the "Hold Off Print Job" setting

By default HP devices have a 15 second delay to start printing network print jobs when someone is using the device (e.g. logged in to the device LCD).   This can cause a 15 second delay to print jobs when a user releases a job from a hold/release queue.

This setting may be disabled either through the device LCD or through admin web interface. To disable via the admin web interface:

*   Login to the device web interface as admin.
*   Navigate to General -> Control Panel Administrative Menu -> Administration -> General Settings
*   Change the "Hold Off Print Job" setting to "Disabled"
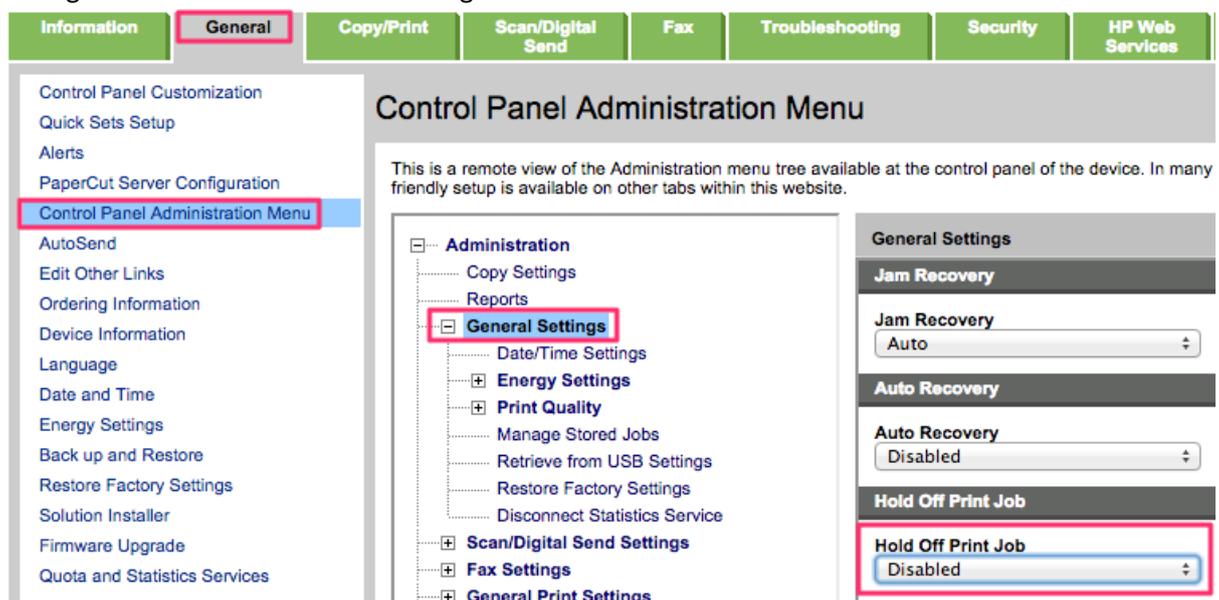
- Press "OK" to save the changes.

3.2.5 PaperCut Settings

1. Using a web browser, log into the PaperCut administration interface (e.g. `http://papercut-server:9191/admin`).

2. Navigate to the Devices tab

   Devices tab not present? See 9.1 The Devices tab is not present.

3. Select the HP device from the list. The Device Name should be the name selected in step 3.2.2.

4. Under the **External Device Settings** section, fill in the values for **Device's administrator username** and **Device's administrator password** . PaperCut requires these to register to the device to receive job information.

5. Additional settings can be applied now, such as the type of jobs to track and the authentication options that will be available.

6. Click Apply.

7. Under **External Device Settings** , monitor the **Device status field** to ensure that PaperCut can successfully connect to and set up the device. After around 20 seconds this field should read `Started`.

3.2.6 Additional Network Security (optional)

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

By default PaperCut will allow device connections from any network address. To restrict this to a subset of IP addresses or subnets:

1. Logon to the PaperCut administration web interface at http://<papercut-server>:9191/admin

2. Go to the Options→Advanced tab and find the "Security" section.

3. In the "Allowed device IP addresses" field enter a comma-separated list of device IP addresses or subnets (in the format <ip-address>/<subnet-mask>).

4. Press the "Apply" button.

5. Test the devices to ensure they can continue to contact the PaperCut server.

3.3 Upgrading to a newer version

The procedure for upgrading an existing embedded application to a newer version is similar to the initial installation (see 3.1.2 through 3.2.3). Please note that only the device-level installation needs to be performed, and you shouldn't have to perform any additional configuration within the PaperCut administrator interface.

After uploading the solution file the device should prompt to restart before installation is complete. Choose Restart Now to restart the device.

4 Post-install testing

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

1. To ensure that the embedded application is working as expected.

2. To familiarize yourself with the features and functionality of PaperCut and the embedded application.

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

4.1 Test Preparation

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

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

If you already have existing users for testing, then there is no need to create the users above. Instead you can use your existing users for testing.

To set up these users in PaperCut:

1. Create the `testusersimple` and `testuseradvanced` users in your Active Directory or LDAP directory.
2. Log into PaperCut admin interface.
3. Navigate to **Options → User/Group sync** and press **Synchronize Now** .
4. Once the sync is complete, the users will be added to PaperCut.

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

1. Navigate to the **Users** tab in the PaperCut admin interface.
2. Select the `testusersimple` user.
3. Set the user's balance to $50.00 and verify the account is set to **Restricted** .
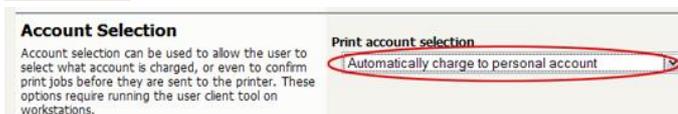

4. Verify that this user is set to **Automatically charge to personal account** under **Account selection** options.

5. Press **OK** to save.

To configure `testuseradvanced`:

1. Navigate to the **Users** tab in the PaperCut admin interface.

2. Select the `testuseradvanced` user.

3. Change the **Account Selection** option to **Standard account selection popup** and enable all the account selection options.

4. Press **OK** to save.

4.2 Scenario 1: Standard copying

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

At the photocopier device:

1. Press **Sign In**.

2. Enter the `testusersimple` username and password and press **OK**.

3. Press **OK** if you see the optional confirmation / "Access Approved" screen.

4. At this point the copier will be enabled for use. Any copying/scanning/faxing performed will be charged to the logged in user.

5. Once completed, press **Sign Out** to return to the front screen.

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

1. Log into PaperCut admin interface.

2. Select the device from the **Devices** tab.

3. Select the **Job Log** tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed. Verify the details of the copy job that was just performed.

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

4. Click on the user's name in the user column to view the user's account details

5. Select the **Job Log** tab to display all print/copy activity for the user.

6. Select the **Transaction History** tab and verify that the cost of the photocopying was deducted from the user's account.

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

4.3 Scenario 2: Copying with account selection

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

First some test accounts should be created:

1. Log into the PaperCut admin interface.
2. Navigate to the **Accounts** tab.
3. Select the **Create a new account…** action link on the left.
4. Enter an account name `Test Account 1`.
5. Press **Apply**.
6. Select the **Security** tab and allow all users to access the new account by adding the `[All Users]` group.
7. Press **OK**.
8. Repeat the process to create another few accounts.

At the photocopier:

1. Press **Sign In**.
2. Enter the `testuseradvanced` username and password and press **OK**.
3. Press **OK** if you see the optional confirmation / "Access Approved" screen.
4. Open the **Account Selection** app on the home screen.
5. The Account Selection app will display a list of shared accounts along with options to search for an account by name or charge to an account by PIN. The options on this page will change depending on the user's account selection settings. Additionally, if the **Make shared account PIN/code visible** option is enabled in PaperCut, searching for an account by its code is also possible.
6. Select the account to allocate copying to. E.g. "Test Account 1".
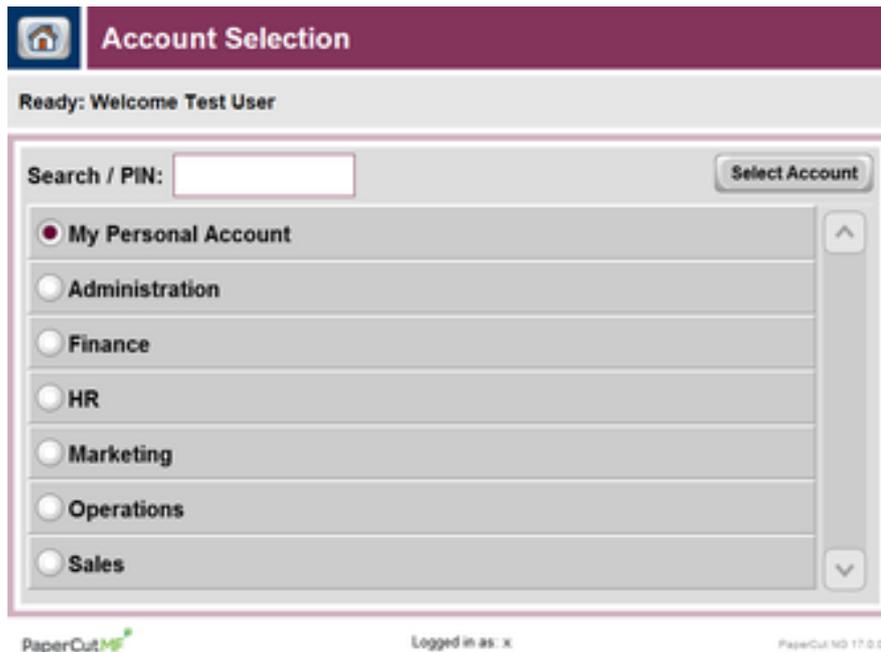
7. Open the **Copy** app on the home screen and perform some test copying.

8. Once completed, press the home button in the top left to return to the home screen then press **Sign Out**.

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

1. Navigate to the **Devices** tab in the PaperCut admin interface.

2. Select the HP MFP being used for testing from the list.

3. Select the **Job Log** tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed.

4. Verify the details of the job (i.e. that the job was charged to the selected account).

5. In the log details, click on the **Charged To** account name to view the account's details.

6. Selecting the **Job Log** tab will display all print/copy activity for the account, and will show the test photocopying that was performed.

4.4 Scenario 3: Print release

The embedded application may also be used for print release. For full description of PaperCut hold/release queues and release stations, please read the PaperCut manual.

Skip this scenario if hold/release queues will not be used at your site.

To perform print release testing, a hold/release queue must be enabled:

1. Navigate to the **Printers** tab in the PaperCut admin interface..

2. Select the print queue (not the device) for the HP MFP being used for testing.

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

☑ Enable hold/release queue

Release mode
User release ▾
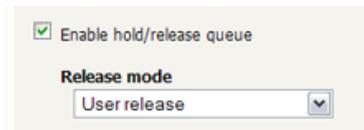
4. Press **Apply** to save the changes. All printing to this queue will now be held until released by a user.

The photocopier device must also be enabled as a "Print Release Station":

1. Navigate to the **Devices** tab in the PaperCut admin interface.

2. Select the HP MFP being used for testing from the list.

3. Under **External Device Settings → Device function** , enable the **print release** option.

4. Under the **Displays jobs for release from the selected queues** option, select the print queue that was enabled for hold/release above.

5. Press **OK** to save the changes. In the **External Device List** the device is now listed as having the **Print Release** function.

6. Log into a workstation as `testusersimple`.

7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.

8. Confirm that the jobs are held by checking that the jobs are listed in the **Printers → Jobs Pending Release** page of the PaperCut admin interface and that the username displayed on this page is `testusersimple`.

At the photocopier device:

1. Press **Sign In** .

2. Enter the `testusersimple` username and password and press **OK** .

3. Press **OK** if you see the optional confirmation / "Access Approved" screen.

4. Select the **Print Release** app from home screen.

5. The list of held print jobs is displayed.
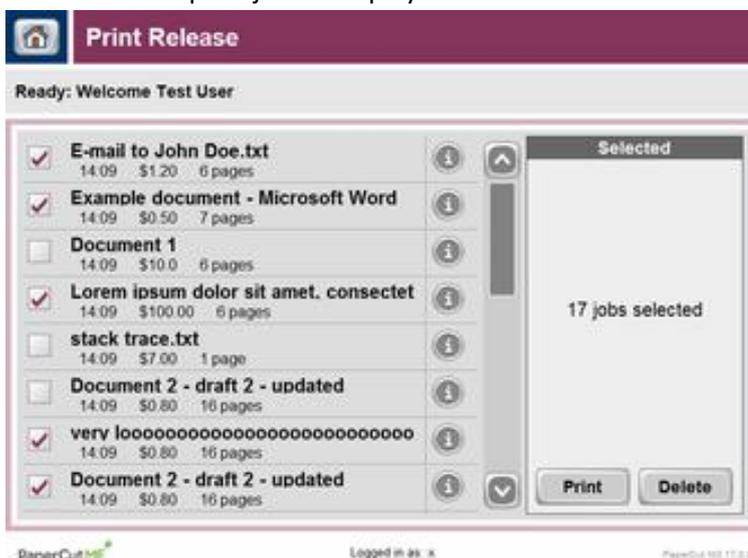
6. Try releasing a single job by pressing the " **i** " icon next to a print job then pressing **Print** on the dialog that appears.
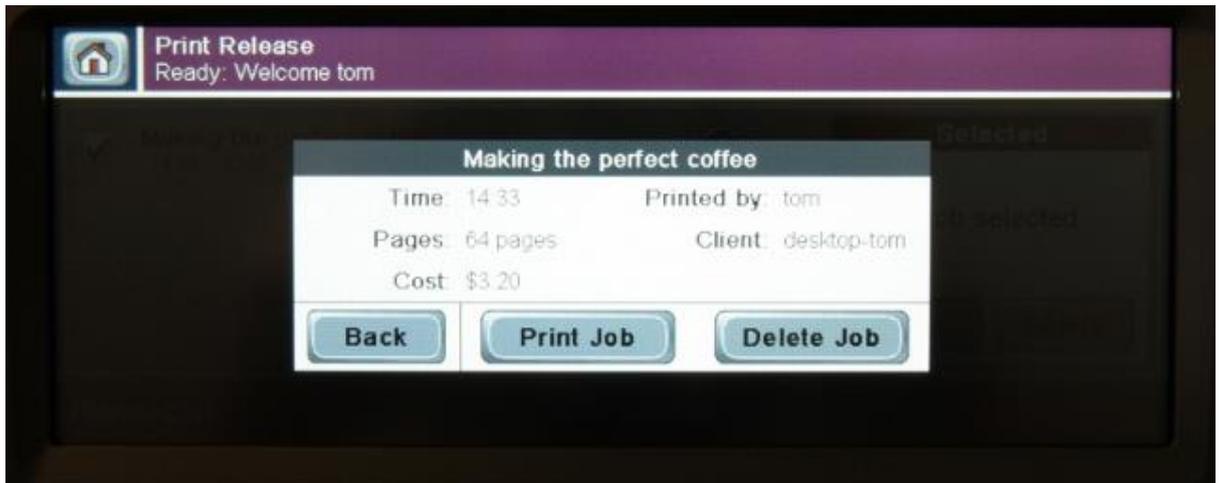
7. The job will then print.
8. Try canceling a single job by pressing the " **i** " icon next to a print job then pressing **Delete** on the dialog that appears.
9. The job will be canceled, and will not print.

5 Configuration

After completing the Installation section and registering the device with PaperCut it will have been configured with reasonable default settings that are suitable for most environments. This section covers how to change the default settings. All the following settings are available via the device's **Summary** tab in the PaperCut admin interface.

5.1 Device Function

The device function settings define which functions will be available on the device and how it will be used. Not all function settings are supported on all devices.

Device Function	Description
Track & control copying	The device will track walk-up off-the-glass copying and on-device printing.
Track & control scanning	The device will track scanning such as scan-to-email or scan-to-file.
Track & control faxing	The device will track the sending of faxes.
Enable print release	The device will act as a print release station.

5.2 Device Options

5.2.1 Confirmation Screen

The confirmation screen is the screen displayed after authentication. It includes the default account to be charged (the personal account, if account selection is not enabled), and the account balance (if the account is restricted).
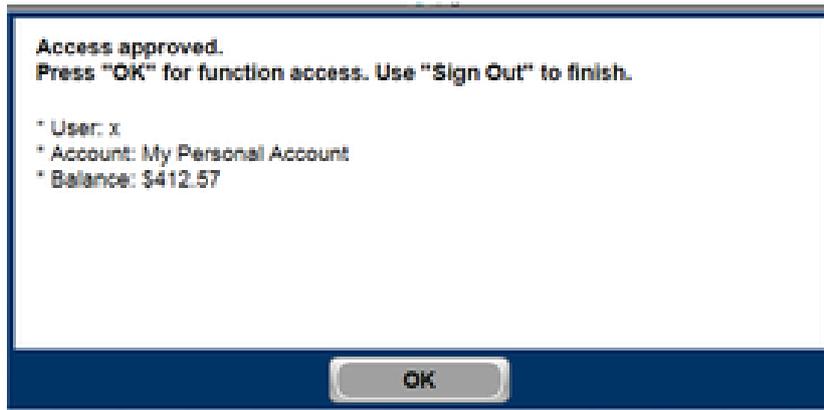
This screen can be disabled by unchecking the option **Show account confirmation** under **Device Options** .
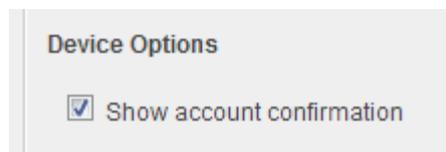
When the confirmation screen is disabled the user is taken directly from authentication to the device's home screen.

5.3 Authentication Methods

PaperCut supports a number of different ways to authenticate users who walk-up to devices to perform copying. The default authentication method is username and password authentication.

The available authentication methods can be modified at **External Device Settings -> Authentication methods** .
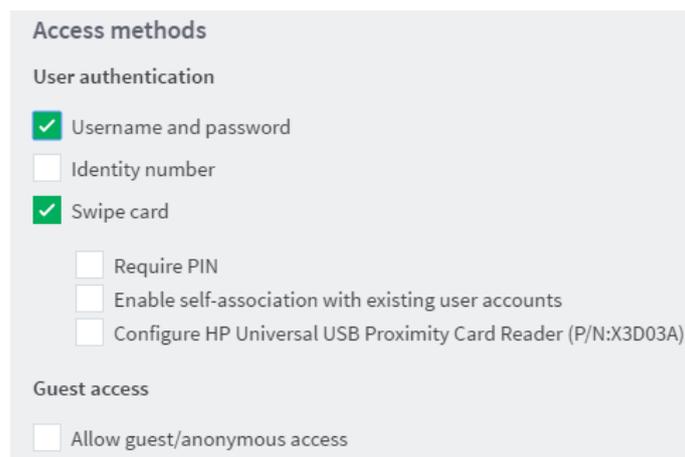
Authentication methods available for a device

Authentication Method	Description

Username and password	The user may use their domain/network username and password to log into the device.
Identity number	The user may log in by entering their id number.
Swipe card	The user may log in by presenting a card (e.g. magnetic strip, smart card, RFID). See the PaperCut user manual for information about user card numbers, including importing card numbers from an external source.
Swipe Card → Enable self-association with existing user accounts	If enabled, when a card number is swiped that is unknown to PaperCut the user will be prompted to associate their card with their user account. To do this, the user must enter their existing username and password. Afterwards, the user may swipe their card to log in.
Swipe Card → Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)	Enabling this, allows you to configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader, from within PaperCut MF, to read the various card types that your users will use. For more information on how to configure your card readers, refer to 6.4.7 HP Universal USB Proximity Card Reader and RF IDeas RDR-805H3AKU.

<center>**Description of authentication methods**</center>

Note that on compatible HP FutureSmart 3 devices, only one of the **Username and password** and **Identity number** authentication options can be enabled at the same time.

5.4 Shared Account Selection

Shared account selection options at the device mirror the options presented in the PaperCut user client's account selections pop-up. The options available include:

- Select from or search a list of shared accounts
- Select or search by shared account code (if using visible shared account codes)
- Select a shared account by PIN (if using hidden shared account PINs)
- Auto-charge to a single shared account (no selection required)

The options available to each user, as well as account security access, will mirror the same options available when the user prints. "Select from list" or "Select using PIN/Code" are both controlled at the user level via the *User Details* page under "Account Selection" when showing the "standard account selection popup". The Security tab on each account controls account security/access.

On compatible HP FutureSmart 3 devices, the **Default shared account** option takes effect by displaying at the top of the list of shared accounts.

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.register.account-selection.** For more information, see 6.1 Config Editor.

5.5 Email Configuration

PaperCut can provide compatible HP FutureSmart 3 devices with user email addresses for use with the "Send to E-mail" functionality. PaperCut will provide a device with a user's email address at login whenever it is available (see *System Notifications and Emailing* in the PaperCut manual).

To control how the device makes use of the user's email address, log into the device's EWS and navigate to **Scan/Digital Send → E-mail Setup → Address and Message Field Control** . Settings include:

- Setting the default **From** address to the user's email or to a fixed address.

- Setting the default **To** address to the user's email or to a fixed address.

- Controlling whether or not the user can edit the email addresses, and if they can edit then whether or not they need to be present in the device's address book first.
- Various other email settings.

6 Advanced Configuration

6.1 Config Editor

The common configuration options for a device in the PaperCut administration interface are available on the device's 'Summary' tab, and are discussed in more detail in the Configuration section. This section covers the more advanced or less common configuration options, which are available via the 'Advanced Config' tab in the device details screen.

Config name	Description
ext-device.card-no-regex	See section 6.4.2.
ext-device.card-self-association.use-secondary-card-number	Select whether user self-association should occupy the primary or secondary card number. It overrides the global setting unless the keyword "GLOBAL" is specified. This is useful when there is a mix of different non-configurable card readers that read different numbers from an ID card. Set to "Y" to use the secondary card number, "N" to use the primary card number. Default: "GLOBAL" to defer to the global configuration option.
ext-device.hp.locale-override	Used to override the language displayed on the device. This may be a 2-letter language code, e.g. "es" for Spanish, or both language and region, e.g. "es_ES" for Spanish in Spain.
ext-device.hp.soap.inbound.use-ssl	The HP device sends SOAP messages to the PaperCut server over HTTP (unencrypted) by default. To send messages over HTTPS/SSL, set this option to "Y".
ext-device.hp.network.timeout-millis	Specify the interval of time (milliseconds) that the device will wait to establish a successful network connection with (and receive a response from) the PaperCut MF Application Server, after which the PaperCut MF Application Server is classified as being timed-out. **Note:** The value of this setting determines the amount of time that it will take for the device to detect that the PaperCut MF Application Server has timed-out. This is a device-specific config key.

Values: 500-60000 (milliseconds)

Default: 5000 (milliseconds)

ext-device.hp.network.timeout-retries	Specify the number of attempts that the device will make to re-establish a successful network connection with (and receive a response from) a timed-out PaperCut MF Application Server. This is a device-specific config key. Values: 0-50 Default: 0
ext-device.hp.windows-domain	Specify the Windows Domain that is used by the device (along with the user's username) to authorize user access to shared drives on your Windows network while saving a scanned file using the native scan-to-network functionality. This is a device-specific config key. Values: Windows Domain Default: N/A
ext-device.hp.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 5.4 Shared Account Selection.
ext-device.hp.restricted.multiple-txns	Specify 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 permitted), Y (multiple transactions not 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.

6.2 Setting an Explicit PaperCut Server Network Address

The device makes inbound network connections to the PaperCut server (for job event notifications) using a network address of the PaperCut server. By default PaperCut will use the server's IP address (if the server has multiple IPs, i.e. multi-homed, then PaperCut will select one of them), but on some networks this address may not be publicly accessible from other parts of the network.

If the PaperCut server has a "public" IP address or DNS name then this can be used instead. To do this:

- Navigate to the **Options → Config editor (advanced)** in the PaperCut admin interface.
- Find the "`system.network-address`" setting.
- Enter the public network address for the PaperCut server.
- Press **Update** next to the setting and confirm the setting is updated.

When connecting devices to a PaperCut site server, you can configure the sites' **Network address used by devices** :

- Navigate to the **Sites** tab in the PaperCut admin interface.
- Select the site to edit.
- Change the **Network address used by devices** .
- Save the site details.

To have either of these changes take effect immediately, restart the PaperCut application service (i.e. on Windows use **Control Panel → Administrative Tools → Services**).

6.3 Session Inactivity Timeout

Once a user has logged into an HP FutureSmart device they will be logged out automatically if they do not perform any activity for 60 seconds.

This timeout value can be changed in the device's web admin at **General → Control Panel Administration Menu → Administration → Display Settings → Inactivity Timeout** (at the time of writing this setting cannot be controlled by PaperCut).

6.4 Configuring Card Readers for Authentication

Authentication cards contain numbers which are used to identify users according to the card number configured in PaperCut (**Card/Identity Number** on the **User Details** page for a user).

Some readers report information in addition to the number encoded on the card, such as checksums. PaperCut can treat these cases in two ways:

6.4.1 Card Number Needs No Conversion

- A typical case is the checksum being reported after the card number, separated by an equals sign, such as in `5235092385=8`. PaperCut can handle this case by default; it will extract the number before the equal sign as the card number: `5235092385`.

6.4.2 Regular Expression Filters

- For some cases, a "regular expression" *may* be required that will filter the card number from the complete string of characters reported by the card reader. Documentation on regular expressions can be found on the Internet, e.g. at www.regular-expressions.info.
  - The regular expression must be fashioned so that the card number is returned as the first match group.
  - Usually one regular expression will be used for all the devices managed by PaperCut; this must be entered at **Options → Actions →Config editor (advanced)** using the key "`ext-device.card-no-regex`".
  - The global setting however can be overridden on a per-device basis: The key "`ext-device.card-no-regex`" can also be found on the **Advanced Config** of the device. This setting will override the global setting unless the keyword "`GLOBAL`" is used.
  - PaperCut support will gladly assist in producing a regular expression when supplied with a few sample outputs from your card reader. Contact your reseller or Authorized Solution Center for help with regular expressions. You can find their contact information in your PaperCut Admin interface on the **About** page.
  - If you would like to write your own regular expressions, here are some examples:
    - Use the first 10 characters (any character): `(.{10})`
    - Use the first 19 digits: `(\d{19})`
    - Extract the digits from between the two "=" characters in "`123453=292929=1221`": `\d*=(\d*)=\d*`

6.4.3 Card Number Format Converters

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

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

- **Options → Actions → Config editor (advanced)**
- Search for "`ext-device.card-no-converter`"
- Enter the name of the required converter (see table below) and click **Update**.

To set at the device level:

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

6.4.4 Standard Converters

Convertor	Description
`hex2dec`	Convert a hexadecimal (base 16) encoded card number to decimal format. Hexadecimal numbers usually contain 0-9 and A-F. This will convert "`946EBD28`" to "`2490285352`".
`dec2hex`	Convert a decimal encoded card number to hexadecimal format. This will convert "`2490285352`" to "`946EBD28`".
`ascii-enc`	Unpack an ASCII encoded card number string. E.g. given the number "`3934364542443238`", the ASCII code "`39`" is converted to `9`, "`34`" -> `4`, "`45`" -> `E`, with the entire number resulting in "`946EBD28`".
`javascript:<path>`	Advanced: Define a custom conversion function in JavaScript (see below)

It is possible to chain or pipeline converters by delimiting with a pipe (|). For example, `ascii-enc|hex2dec` will first unpack the encoded ASCII number then convert it to a decimal.

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

6.4.5 Using custom JavaScript

If the inbuilt converter functions are unable to meet the requirements, it is possible to define your own function using JavaScript. This is an advanced exercise and it is expected that any implementer be familiar with programming and JavaScript. To implement your own converter:

1. Create a file text file `[install-path]/server/custom/card.js`
2. Define a single JavaScript function in this file called "`convert`". It should accept and return a single string. Here is a trivial example:
   ```
   function convert(cardNumber) {
     return cardNumber.substring(3,10).toLowerCase();
   }
   ```
3. Enter a converter in the form: `javascript:custom/card.js`

Tip: Check the file `[install-path]/server/log/server.log` when testing. Any scripting errors will be displayed as warning messages in the log.

Tip: A JavaScript script may also be included in the pipeline. For example "`ascii-enc|hex2dec|javascript:custom/card.js`".
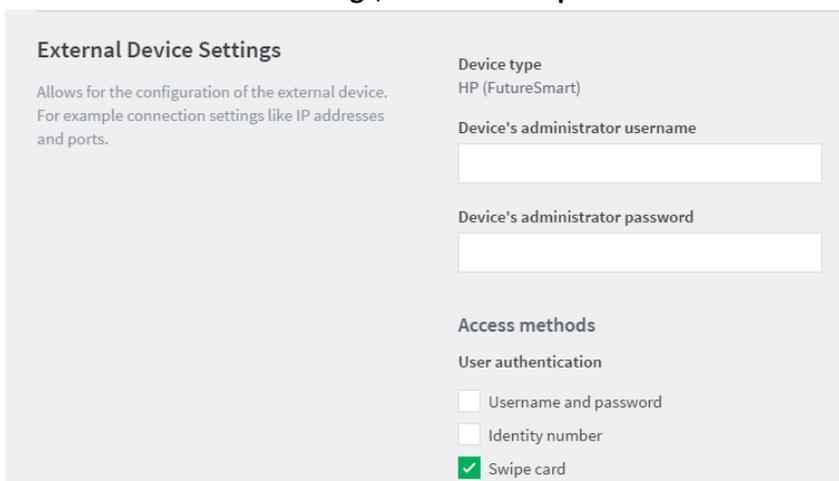
6.4.6 Other advanced notes

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

6.4.7 HP Universal USB Proximity Card Reader and RF IDeas RDR-805H3AKU

If you enable the **Swipe card** authentication method and you use the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader, then you must configure it.

To configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader:

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:

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

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:

- You can configure up to four card types:

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

Card type #1	
MiFare Ultralight CSN (Philips, NXP)	v

Card type #2	
HID Prox	v

Card type #3	
-- Not Configured --	v

Card type #4	
-- Not Configured --	v

- Some card types conflict with other card types. Hence, avoid selecting such conflicting card types, because this causes some problems when using swipe card authentication for logging in and self-association.

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

6.4.8 Scan to Folder with Single Sign On

It is possible to configure the HP FutureSmart device to connect to a UNC path with a specific username and password to enable Scan-To-Folder or Scan-To-Home. This does require that a "service account" is created in your network that has the ability to write to the folder you will specify later. This account should have a very secure password and is not in common use across your environment. It is also advised that this account is restricted from accessing services other than writing to the specified UNC path(s) below.

1. Using a web browser, navigate to the HP device's web admin, e.g. **http://staff-room-hp/**

    and click **Sign In** in the top-right corner of the page and sign in as a device administrator.

2. Navigate to **Scan/Digital Send -> Save to Network Folder Setup**

3. Click **Add** under **Quick Sets**

4. Use a meaningful **Quick Set Title** such as **Colour PDF**, a descriptive **Quick Set Description** and select the **Button Location** most appropriate for your organization and click **Next**.

5. Select **Save to shared folders or FTP folders** and click **Add**.

6. On the **Quick Set Wizard** page enter a valid UNC path which is available to the service account you have previous created. A feature here is you can configure a **Custom Subfolder** that includes the logged in username. This would mean the service account needs write permission to this location.

    You can use the **Update Preview** button to confirm what the full path will consist of. Make sure to remove any double slashes.

    You may want to designate a sub-folder in each user's home directory as the destination. This will need to be pre-created.

    Select **Always use these credentials** and input the Windows Domain, Username and Password of the service account and click **Verify Access** to confirm everything is working as expected.

7. Click **OK**.

8. Select **Next.**

9. Configure the Notification Settings as desired.

   Note: The Notification E-mail Address cannot be left blank, however if the E-mail address of the User is known to PaperCut it will be used instead of the address filled used here.
   Click **Next**.

10. On the Scan Settings page set the default scanning options as desired. Click **Next**.

11. On the File Settings page set the desired default settings. Click **Next**.

12. Confirm the settings on the Summary page and click **Finish**.

7 Known Limitations and Security

7.1 Usability and User Interface Limitations

The HP FutureSmart SDK provides limited ability to customize screens during the device login process and workflow. The login screens are of a fixed design and little can be done to visually enhance them. To provide a richer experience for account selection and print release PaperCut uses the device's web browser via a button on the home. This means that the user is not prompted to perform account selection or print release during login. This is a post-login step.

7.2 Zero-stop when copying

Ideally PaperCut would be able to control exactly how many pages a user can copy and always prevent the user from overdrawing their account. The HP FutureSmart SDK (as of October 2012) offers the ability to limit page counts but copying does not stop immediately when limits are reached. A delay at this point means that users may overrun their account below zero by about 8 sheets (8 pages single-sided, 16 pages double-sided). This time delay to stop has been raised with HP and any changes will be updated here. This is outlined on the Known Issues with HP FutureSmart Embedded App (PaperCut MF) page.

If you are interested in seeing a "strict zero stop" mode added where users are unable to start any job if they do not have enough credit to print at least 8 sheets of the largest supported paper size (i.e. removing any chance of an overrun), contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.

7.3 Bypassing the System

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

- The copier's built in admin password should be changed and always kept secure.

See section "8.1: Temporarily Disable PaperCut" to see how an administrator can temporarily bypass PaperCut.

8 Uninstalling PaperCut from the Device

8.1 Temporarily Disable PaperCut

In order to stop the HP MFP from trying to authenticate with PaperCut and to allow free copying on the device, the following procedure can be followed:

1. Log into the HP FutureSmart device's web admin using the administration credentials

2. Navigate to **Security → Access Control** .

3. Click the checkbox below the **Device Guest** column header.
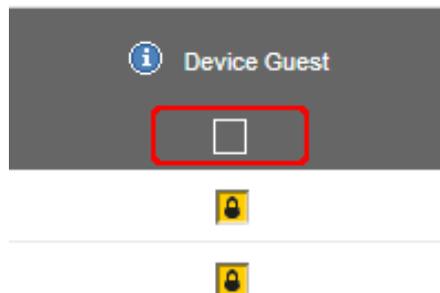
   This should result in all the locks in that column changing to ticks. This means that users who are not logged in can access any device function, and the default screen will become the home screen (i.e. not the "welcome" sign-in screen).

4. Click **Apply** to save the settings.

5. Navigate to **General → Quota and Statistics Services** .

6. Uncheck the option **Connect this device to a Quota Server** . This will disable tracking and limiting of copy/scan/fax jobs at this device.

7. Click **Apply** to save the settings.

The device can be re-enabled by reversing the process (icons in the **Device Guest** column should appear as locks, **Quota Server** option should be enabled).

8.2 Full Uninstall

1. Log into the HP FutureSmart device's web admin and navigate to **General → Solution Installer** .
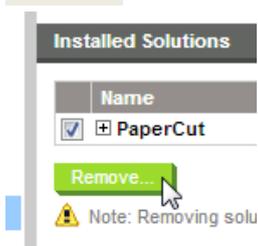
2. Select the **PaperCut** row and click **Remove…** .

3. The device will reboot to complete the uninstallation.

9 FAQ & Troubleshooting

9.1 The Devices tab is not present

If the Devices tab is not visible in the PaperCut admin interface next to the Printers tab then External Hardware Integration might be disabled. To enable External Hardware Integration:

1. Using a web browser, log into the PaperCut administration interface (e.g. `http://papercut-server:9191/admin`).

2. Navigate to Options → Advanced and ensure the option Enable external hardware integration is enabled.

3. Click Apply.

9.2 A user has overrun their quota during a copy job. Why didn't it stop them earlier?

Device limitations mean that copy jobs can overrun their quota by up to 8 sheets.

9.3 The device displays the home screen when nobody is logged in (and the Sign Out button says Sign In)

This is a device feature called "lazy authentication". If the Guest user profile on the device has access to any device function, the home screen (with the app icons) will become the default screen instead of the Sign In screen. PaperCut will attempt to lock down access to all device functions when the embedded app is installed, but it is possible (e.g. by an administrator manually changing settings) to go back into lazy authentication mode.

Note that to allow color printing the "Print in Color" option must be allowed for guest users, and doing this will enable lazy authentication.

To disable lazy authentication and display the Sign In screen by default:

1. Log into the HP FutureSmart device's web admin using the administration credentials

2. Navigate to Security → Access Control .

3. Click the checkbox below the Device Guest column header until all icons in that column change to locks.

4. Click Apply to save the settings.

9.4 What is the IP address of my PaperCut Server?

Use the operating system's command-line tools such as ipconfig or ifconfig to determine this.

9.5 I have thousands of accounts representing my clients. Will the system handle this?

Yes, we have designed the system to handle thousands of shared accounts.

9.6 I have configured color copying restrictions in PaperCut, but all users are still able to copy in color. Why?

Make sure the steps from section *3.2.3 Configure Device Access Control* have been followed.

9.7 When I click the Print Release button I receive a OXPd Application Error

This is caused by a security function on the copier itself called "CORS". You can configure this via **Security → Web Service Security** .

You can either disable this functionality or add the IP address subnet of the PaperCut Application Server to the "Trusted Sites".

Make sure to click **Apply** when finished.

10 Appendix A: Supported Authentication Card Readers

PaperCut MF - HP FutureSmart Legacy supports the following card readers on HP FutureSmart 3 devices:

| Card Reader Type (USB) |
| --- |
| Elatec TWN3 HID Prox |
| Elatec TWN3 iCLASS |
| Elatec TWN3 MIFARE |
| Elatec TWN4 (HID Prox, iCLASS, MIFARE) |
| HID OMNIKEY 5427 |
| HP Common Card Reader (model CZ208A) |
| HP Universal USB Proximity Card Reader (Part Number X3D03A) |
| Magtek magstripe |
| RFIDeas iCLASS |
| RFIDeas magstripe |
| RF IDeas RDR-805H3AKU |

11 Appendix B: Device screenshots for user documentation

This section contains some screenshots that may be used for end-user documentation.

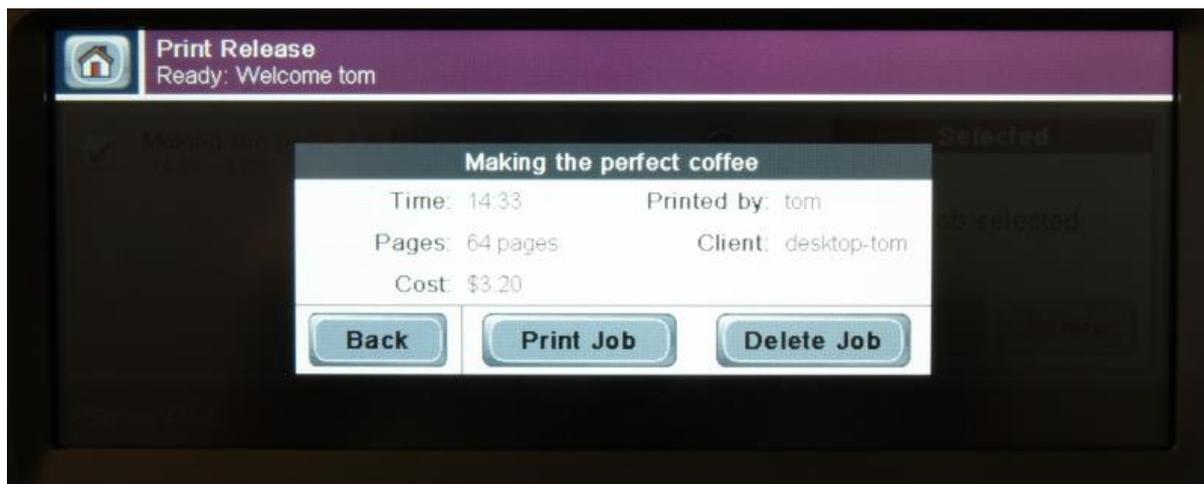Welcome / signin (default) screen:
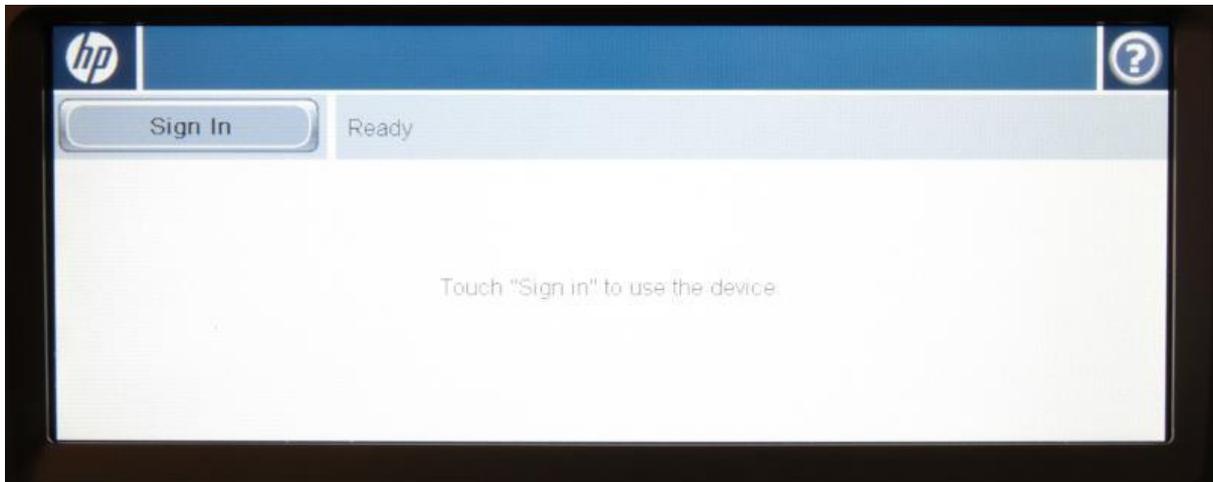
Confirmation screen showing personal account and balance (optional screen):
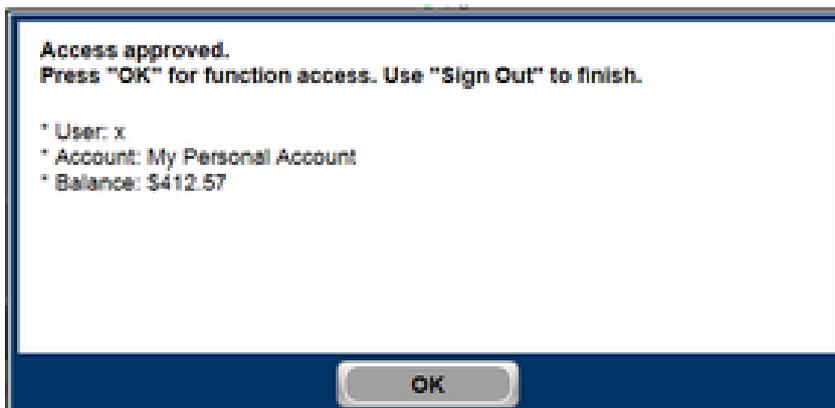
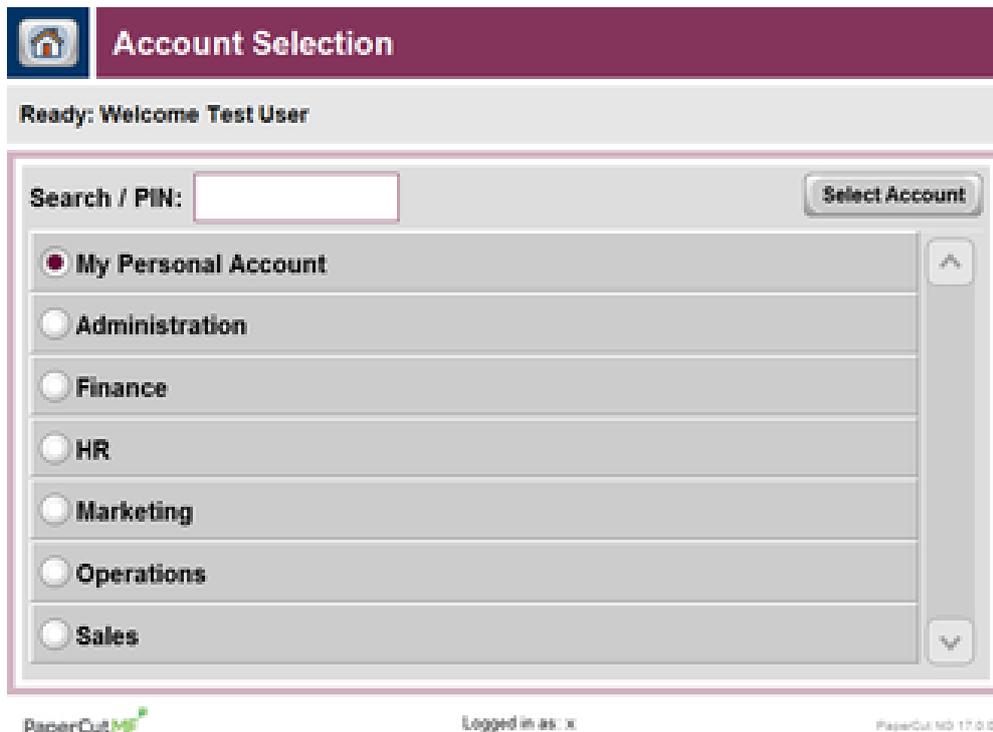Print release screen showing jobs awaiting release:

Releasing a single job (after clicking an " **i** " icon):

Print release screen when there are no jobs awaiting release:

Print Release

Ready: Welcome Test User

You have no jobs awaiting release

New jobs will appear here automatically.

PaperCut MF   Logged in as : x   PaperCut MD 17.0.0

Shared account search / selection screen.

Account Selection

Ready: Welcome Test User

Search / PIN: [   ]   Select Account

● My Personal Account   ∧

○ Administration

○ Finance

○ HR

○ Marketing

○ Operations

○ Sales   ∨

PaperCut MF   Logged in as : x   PaperCut MD 17.0.0

User card association: