PaperCut Canon Embedded Manual

Contents

This manual covers the PaperCut MF Canon embedded setup. For general PaperCut MF documentation, please see the [PaperCut MF manual](#).

1 Overview

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, scanning and faxing (quotas, charging, allocation and logging)
- Allocation of copying, scanning and faxing to accounts/departments/cost-centers/projects
- Release jobs from a hold/release queue (Secure & Find Me Printing)
- Group based access control: Limit access to color copying, the device as a whole, or to selected user groups
- Self-associate swipe cards with domain user accounts directly at the device
- Streamlined interface throughout
- Self-association and print release are possible as part of the device login
- Account invoice and comment options are supported
- Customizability of print release and account selection screens
- Logo, messages and colors are customizable

Highlights of the embedded solution include:

1.1 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.

1.2 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.

1.3 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 as regularly as software updates.

1.4 Vendor Neutral

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

1.5 Security

A large percentage of PaperCut's user base is in educational environments where security is important. All embedded solutions are developed with security in mind. Where security objectives cannot be satisfied, the deficiencies are fully disclosed.

1.4 Vendor Neutral

2 Installation Requirements

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

2.1 Requirements

Before installing the PaperCut Embedded Application on to the Canon device, ensure that basic monitoring of network printing has been setup up and tested for this device. The device would show up in the printer list in the PaperCut web interface and have a few print jobs in its print history.

After that, ensure that the following points are checked off before getting started:

- PaperCut is installed and running on your network. Please see the 'Introduction -> Quick Start Guide' section of the PaperCut user manual for assistance.
- Ensure that your Canon device is supported.
- Ensure that the Canon device is connected to the network.
- Have available the network name or IP address of the Canon device.
- It is recommended that the device be configured with a *static IP address*.
- Verify that firewalls or other network restrictions do not prevent the device's access to the PaperCut server on ports 9191, 9192 and 9193.

2.2 Device Type Compatibility

Integration is supported for compatible Canon Multi-Function Devices (MFDs). For a list of supported models, see http://www.papercut.com/tour/embedded/canon#supported.

Please check with your local Canon supplier that your devices are running an up to date firmware version.

3 Installation and Setup

The following installation steps are based on the Canon iR-ADV C5240 of the Canon Grasmere Series of MFDs. The administration web interface and steps may differ for your model.

3.1 Mandatory Device Configuration

Please access the remote UI at `http://<device-ip-address>:8000` and login as the administrator.
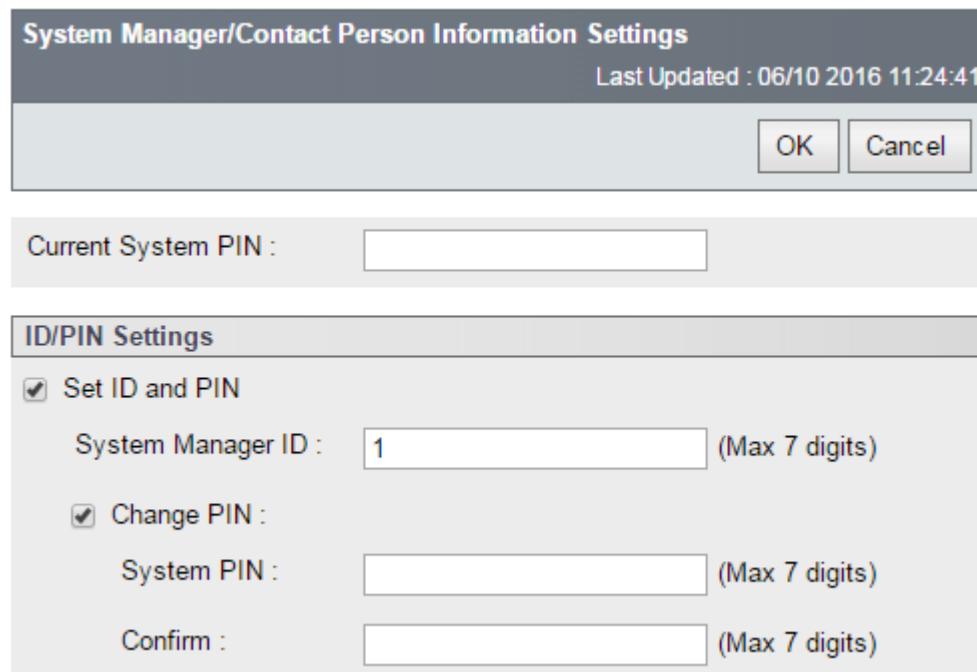
3.1.1 System Manager ID/PIN

The PaperCut application uses ID/PIN System Manager authentication for compatibility with all the supported Canon devices. Ensure the System Manager ID/PIN is configured *before* installing PaperCut on the device:

1. Select **Settings/Registration** .

2. Select **User Management** .

3. Select **System Manager/Contact Person Information Settings** .

.

4. Select **Set ID and PIN** ; then enter the **System Manager ID** and **PIN** .

5. Select **Change PIN** ; then enter the **System PIN** .

6. Click **OK** .

3.1.2 Enable Job logging

For PaperCut to track activity on a Canon MFD requires access to the device's job logs. From the remote UI:

1. Select **Settings/Registration**

2. Select **Device Management** (under **Management Settings**)

3. Select **Display Log**

4. Check **Obtain Job Log from Management Software** and click **OK**
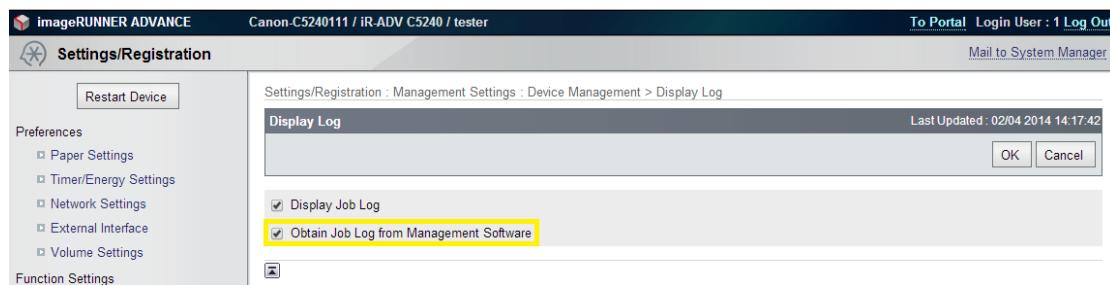
3.2 Optional Device Configuration

3.2.1 Enable USB Input for Card Readers and Storage Devices

If connecting a USB card reader or storage device to the MFD (but not a USB keyboard):

1. Select **Settings/Registration.**

2. Select **External Interface** (under **Preferences**).

3. Select **USB Settings.**

4. Check **Use as USB Device.**

5. Check **Use MEAP driver for USB Input Device.**

6. Uncheck **Use MEAP driver for External USB Device.**

7. Click **OK.**
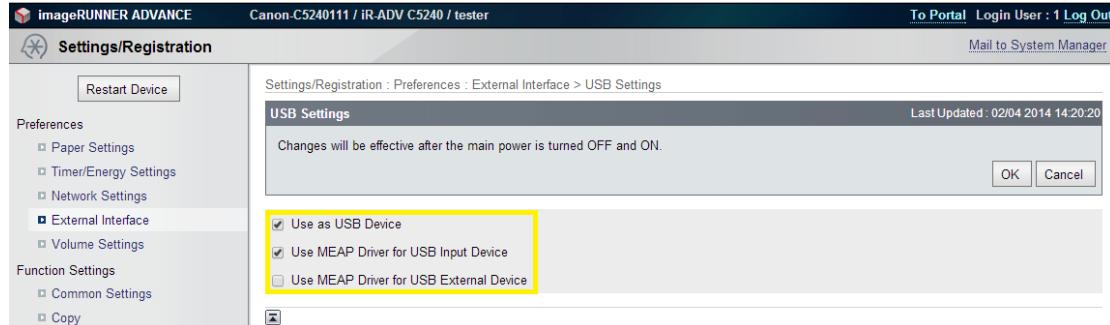
3.2.2 Enable USB Input for Keyboards, Card Readers and Storage Devices

If a USB keyboard or storage device is to be connected to the MFD:

1. Select Settings/Registration
2. Select External Interface (under Preferences)
3. Select USB Settings
4. Check Use as USB Device
5. Uncheck Use MEAP driver for USB Input Device
6. Uncheck Use MEAP driver for External USB Device
7. Click OK
8. Reboot the MFD for the changes to be applied.

If a card reader is to be connected to the MFD, it will need to be registered as a card reading input device. Otherwise it will behave as a standard USB keyboard.

1. Obtain the "VendorID:ProductID" of the card reader e.g. 09d8:0310.
2. Log in to the PaperCut server and edit the MFD's config key 'ext-device.canon.card-reader-ids':

Name ▲	Value		
ext-device.canon.card-reader-ids	09d8:0310,09d8:0410,0c27:3bfa	Update	Remove

3. Add the card reader ID to the comma-separated list (if it isn't already) and 'Update' the key.
4. Connect the card reader to the MFD.
5. Log on to the MFD's administration page to confirm the card reader has been registered at `https://<device-ip-address>:8443/sms/` by looking for a request to reboot the MFD:

MEAP Application Management	Updated On:	↻

⚠ You need to restart the device to have driver settings of the USB device take effect.

6. Reboot the MFD to test the card reader.

Note: You must enable the swipe card reader in PaperCut MF:

1. In the PaperCut MF Admin interface, select **Devices**.
2. Select a device.
3. In the **External Device Settings** area, under **Authentication methods**, select the **Swipe card** check box.
4. Click **OK**.

3.2.3 Automatic Log Out

Canon devices have an 'Auto Reset' feature, which by default logs a user out after two minutes of inactivity. The time out length can be modified via the web interface:

1. Select **Settings/Registration**
2. Select **Timer/Energy Settings** (under **Preferences**)
3. Select **Timer/Energy Settings**
4. Configure the **Auto Reset Time**
5. Click **OK**

3.2.4 Status Monitor/Cancel Screen

By default, the 'Status Monitor/Cancel Screen' can be displayed at any time by pressing the 'Status Monitor/Cancel' hard key. This screen can contain sensitive data such as usernames, e-mail addresses, document names etc. This information can be prevented from being displayed by disabling the following setting in the device's web interface:

1. Select **Settings/Registration**
2. Select **Device Management** (under **Management Settings**)
3. Select **Display Log**
4. Turn off **Display Job Log**
5. Click **OK**

If you would like the 'Status Monitor/Cancel Screen' to be unavailable until a user logs in:

1. Select **Settings/Registration**
2. Select **Device Management** (under **Management Settings**)
3. Select **Display Job Status Before Authentication**
4. Turn off **Display Job Status Before Authentication**
5. Click **OK**

3.2.5 Managing USB Storage Media

Canon devices enable printing from USB storage media and scanning to USB media. This functionality can be configured via the web interface:

1. Select **Settings/Registration**

2. Select **Store/Access Files** (under **Function Settings**)

3. Select **Memory Media Settings**

4. Configure **Use Scan Function** and **Use Print Function**

5. Click **OK**

Any changes will require a reboot of the device.

3.2.6 Access Management System (AMS)

The Access Management System allows PaperCut to restrict color copying to selected user groups. AMS is standard for third generation devices, and optional for first and second generation devices. When AMS is installed, you can enable it with the following steps in the device's web portal:

1. Select Settings/Registration.
2. Select Management Settings -> License/Other.
3. Select ACCESS MANAGEMENT SYSTEM Settings.
4. Check Use ACCESS MANAGEMENT SYSTEM.
5. Press OK.

3.2.7 Scan To Email SMTP Settings

If you want to do scanning to email on the device, you can optionally change the following setting to prevent the device from asking for SMTP verification:

NOTE: Due to minor software differences, for some devices the following steps might be incorrect. If you're unable to find the correct setting on your Canon web UI, contact your reseller or Authorized Solution Center for assistance. You can find their contact information in your PaperCut Admin interface on the **About** page.

1. Select **Settings/Registration**

2. Select **Common Settings** (under **Function Settings**)

3. Select **Set Authentication Method**

4. Configure **Information Used for SMTP Server Authentication** and select **Device Settings**

5. Click **OK**

3.3 Embedded Application Installation

Canon use a variety of region specific delivery methods designed to streamline the installation process. Look in the following sub-directory to find out how this is achieved for your region:
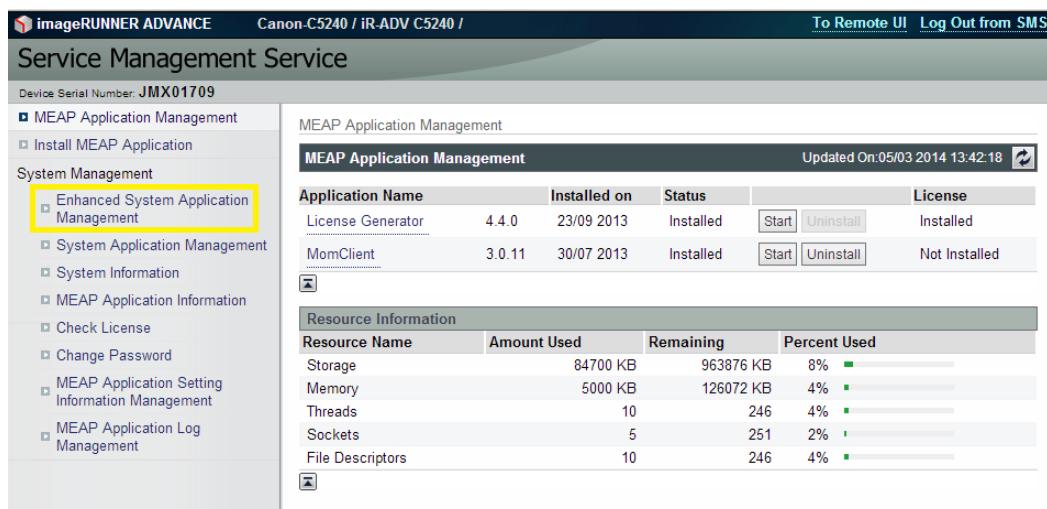
```
[app-path]\providers\hardware\canon\<your-region>
```

The sub-directory will contain either a JAR file, or installation instructions specific to your device's region. The inclusion of a JAR file means you can manually install the application onto the device when coupled with an application license from your Canon dealer.

Speak with your Authorized Solution Center (ASC) representative for further details.

Following are the steps required to manually install the JAR for your region:

1. Log on to the device's administration page, known as the Service Management Service (SMS), under `https://<device-ip-address>:8443/sms/`. Tip: The default administrator's password is usually "MeapSmsLogin".

2. Once logged in, select the **Enhanced System Application Management** option on the left-hand side.

3. Select the PaperCut embedded software for Canon devices, by pressing the **Enhanced System Application File Path Choose File** button.

4. Locate and select the PaperCut embedded software at `[app-path]\providers\hardware\canon\<your-region>\pc-meap.jar`.

5. Select the License File Path   Choose File button, and provide the location of the dealer supplied license file.

6. Press the Install button.

7. You will be asked to confirm the installation of the embedded application. Select Yes .

8. When the PaperCut embedded application has been installed, you will be returned to the Enhanced System Application Management page. Switch to the "PaperCut" Login Service by selecting the associated SWITCH button.

9. The "PaperCut" Login Service status will change to "Start after Restart". Restart the device to activate the PaperCut embedded application.

3.4 Application Settings

Once the device has restarted, you can configure the PaperCut embedded application for Canon devices by typing the following URL into a web browser: `http://<ip-address-of-device>:8000`

1. Enter the System Manager ID and System PIN . Tip: By default, they are both "7654321".

2. Press the Configure PaperCut button.

PaperCut Configure PaperCut

Device Name	canon-device
Server IP/Host	hostname
Server Port (HTTP)	9191 (default: 9191)
Server Port (HTTPS/binary)	9192 (default: 9192)

Advanced settings

Locale Override (optional)	
Debug Mode	☐

Save   Cancel

3. Specify the PaperCut **Device Name** .

4. Specify the **Server IP/Host** of the PaperCut server.

5. Press the **Save** button. The device will attempt to connect to the PaperCut server.

6. Once successfully connected you may need to accept the server's SSL certificate. If so, a notification screen will be displayed on the device.

PaperCut MF
Server Connection

Unable to make a secure server connection. Administrator action required.

Admin Login   Retry
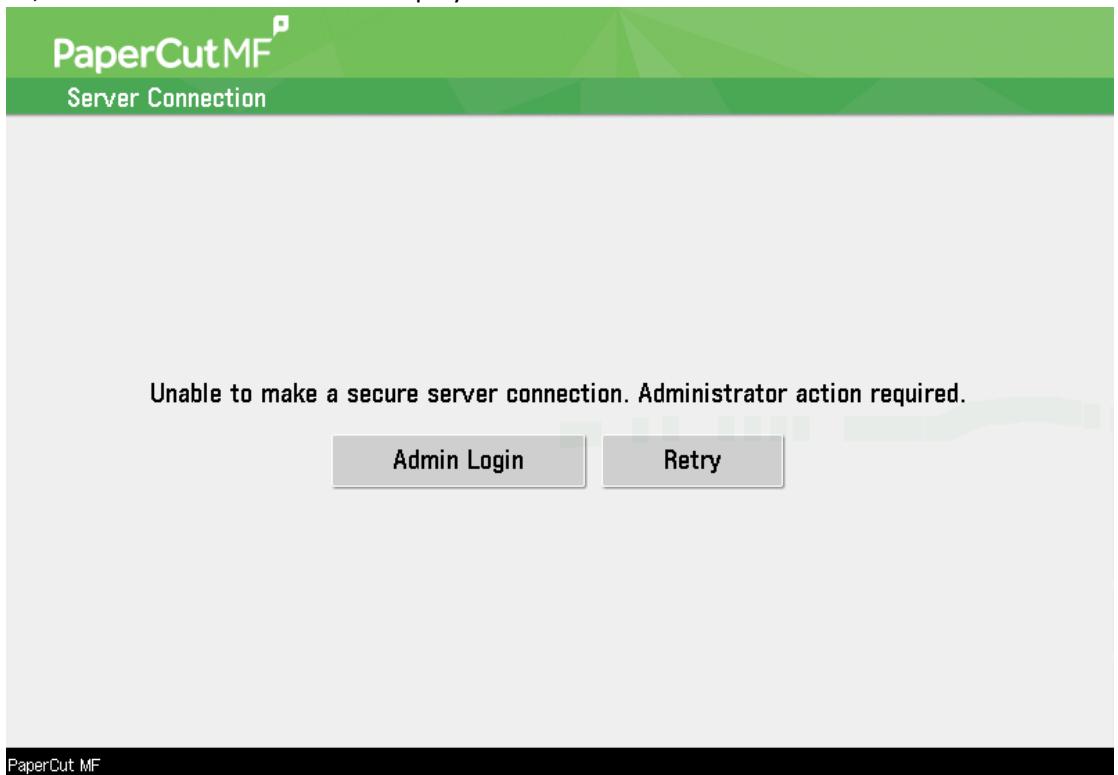
PaperCut MF

7. Log in as the MFD administrator to check that the SHA-1 fingerprint matches the server's certificate.
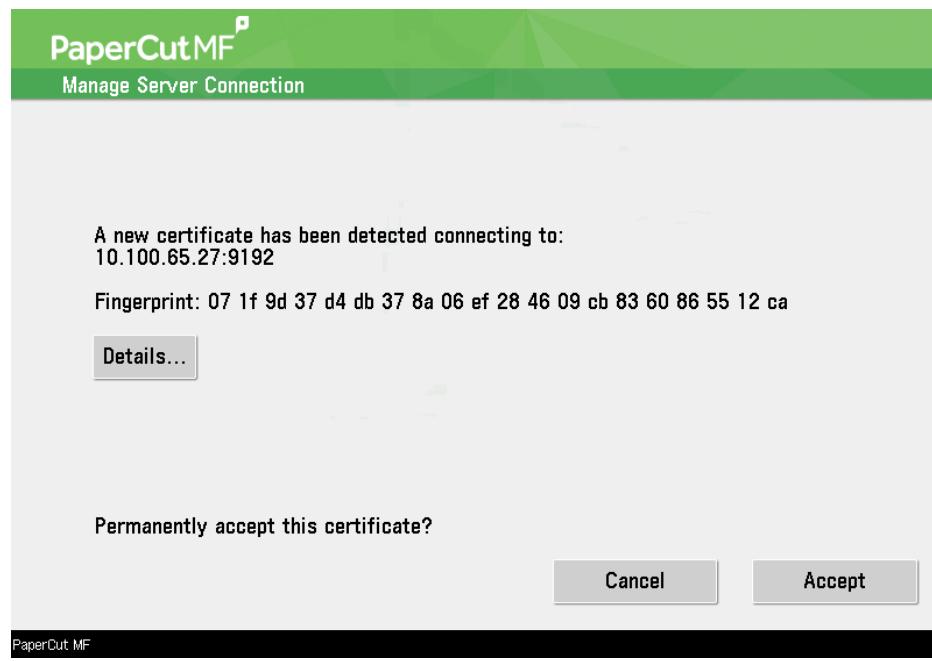
You can also view the certificate details from this screen. See the 'Troubleshooting SSL' section of the PaperCut MF manual for details on viewing server certificates.

8. Press the 'Accept' button to permanently accept the server certificate. The device will attempt to connect to the server with the accepted certificate.

Once the PaperCut embedded application has connected to the PaperCut server, the authentication screen will display on the device, and the MFD will appear in the PaperCut server devices list.
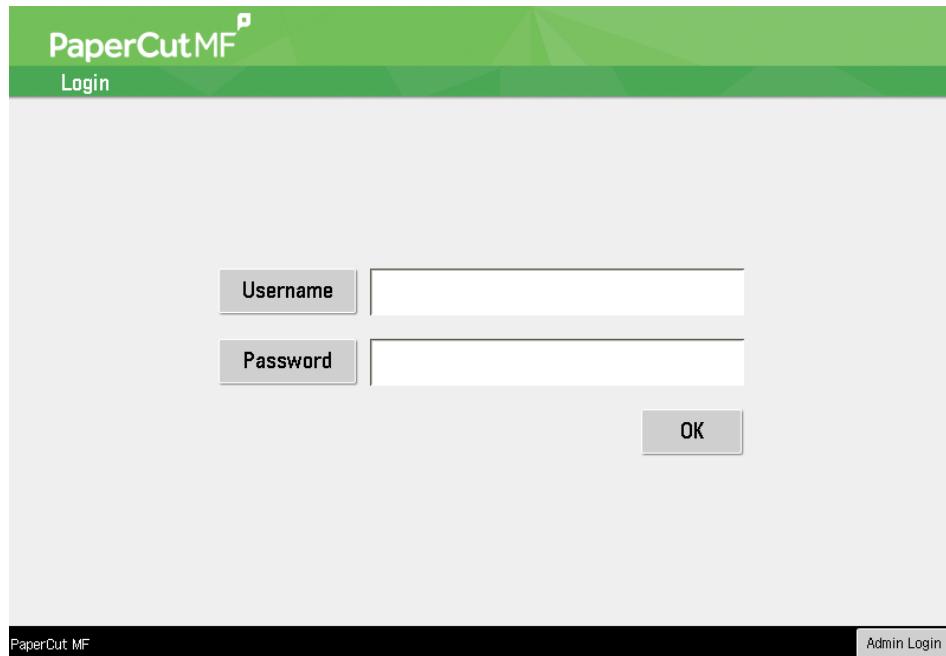
3.5 Additional Network Security (optional)

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 servers

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.

3.6 Card Reader support

PaperCut supports using swipe card for authentication at the copier. This is often more convenient than entering username/password or ID/PIN numbers to log in.

PaperCut supports commonly used keyboard emulating USB card readers including:

- Elatec TWN3 and TWN4
- RF IDeas PcProx Plus
- RF IDeas MS3-00m1aku Mag reader
- NTWare MiCard PLUS
- MiFare and HID iClass Readers

Please ensure the Canon MEAP USB driver is enabled as per the setup instructions in section 3.2.1 above.

4 Upgrading to a newer version

After disabling the embedded application, the procedure for upgrading is the same as the standard installation process, keeping all of your configuration settings.

Note: To upgrade a device with PaperCut application version 1.1.1 or less, to 1.2.0+, you need to uninstall the application rather than upgrading it. There is a known issue where the AMS configurations introduced in 1.2.0 are not applied by devices when they are upgraded from an existing PaperCut version without AMS configurations.

1. Log on to the device's administration page at `https://<device-ip-address>:8443/sms/`.

2. Select the **Enhanced System Application Management** option on the left-hand side.

3. The "PaperCut" login service needs to be disabled before it can be upgraded. Switch to the "Default Authentication" login service by selecting the associated **SWITCH** button.

4. Restart the device and log back into the device administration page as per steps 1 and 2 above.

5. Upgrade the application as per the [Embedded Application Installation](link) instructions.

After upgrading, it's worth checking that the embedded application's version number is correct.

5 Post-install testing

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

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 four test scenarios that are applicable for most organizations. Please complete all the test scenarios relevant for your site.

5.1 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' – used to perform basic copier monitoring and control and to perform print release tests.
- 'testuseradvanced' – 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 have existing users that can be used for these tests, then they can be used instead.

To setup these users in PaperCut:

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

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

1. In PaperCut, select the "Users" tab
2. Select the 'testusersimple' user.
3. Set the user's balance to $50.00 and verify the account is set to "Restricted".
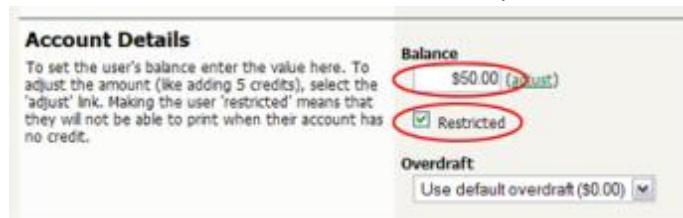
4. Verify that this user is set to "Automatically charge to personal account" in the "Account selection" options.
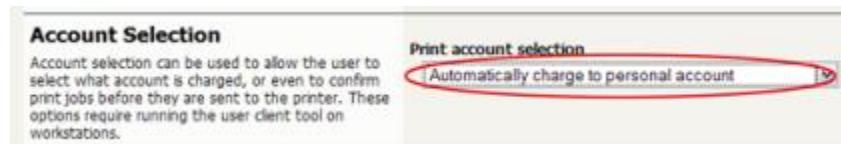
5.   Press the "OK" button to save.

To configure 'testuseradvanced':

1.   In PaperCut, select the "Users" tab
2.   Select the 'testuseradvanced' user.
3.   Change the "Account Selection" option to "Standard account selection popup" and enable all the account selection options.
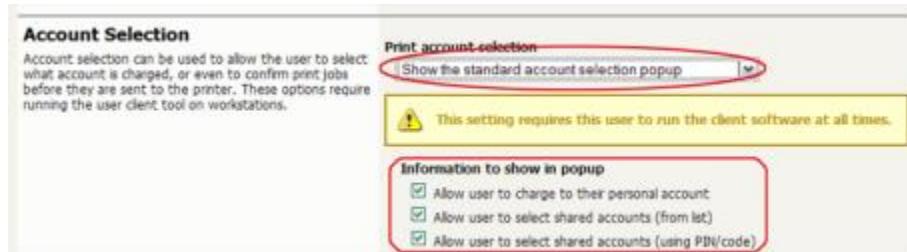
4.   Press the "OK" button to save.

5.2 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/employee use.

At the photocopier:

1.   The photocopier should display a screen to prompt the user to login. Follow the prompts to login.
2.   When prompted, enter username ('testusersimple') and password in the login fields.
3.   At this point the copier will be enabled for usage.
4.   Follow the onscreen instructions and perform some test copying, i.e. press the "Copy" key on the device and perform a copy as normal.
5.   Once completed copying press the "Logout" button on the device's keypad.

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

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

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

4.   Click on the user's name in the user column to view the user's account details
5.   Select the "Job Log" tab to display all print/copy activity for the user.

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

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

5.3 Scenario 2: Copying with account selection

Firstly, a test account should be created:

1. Log into PaperCut, select the "Accounts" tab.
2. Select the "Create a new account…" action link on the left.
3. Enter an account name "Test Account 1".
4. Enter PIN/Code "2233".
5. Select the "Security" tab and allow all users to access that account by adding the "[All Users]" group.
6. Press "OK".

At the photocopier:

1. The photocopier should be displaying a screen to prompt the user to login. Follow the prompts to login.
2. When prompted, enter the username, 'testuseradvanced', and the password in the login fields.
3. You will now be presented with the Account Selection page:

You may select your account from a list, by search or by an account code/PIN. From the list, select the "Test Account 1" created earlier.

4. At this point the copier will be enabled for usage. Follow the onscreen instructions and perform some test copying. I.e. press the "Copy" key on the device and perform a copy as normal.

5. Once completed copying press "Logout" button.

Note: The account selection workflow can vary according to the user options selected. For example, a user configured to see the Advanced Account Selection popup may see an additional dialog asking for comment and invoice information. At the device level, you may also configure whether you wish to see the Account Summary screen or not.

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

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

5.4 Scenario 3: Print release

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

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

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

1. In PaperCut, select the "Printers" tab.
2. Select the print queue (i.e. not the 'device') for the Canon MFD that will be used for testing.
3. Enable the "Hold/release queue" option.

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

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

1. In PaperCut, select the "Devices" tab.
2. Select the Canon MFD device.
3. Under "Device Function" tick "Enable release station".
4. Select the print queue that was enabled for hold/release above. The Canon device will allow jobs on the selected queues to be released.

☑ Enable print release

Displays jobs for release from the selected queues

☑ win7x64-papercu\108 (a 5235)
☐ win7x64-papercu\iR-ADV C2220

5. Press "OK" to save.
6. Login to a computer workstation as 'testusersimple'.
7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
8. Confirm that the jobs are held, by checking that the jobs are listed in the "Printers -> Jobs Pending Release" page of the PaperCut administration interface.
9. Confirm that the username is 'testusersimple'.

At the device:

1. Log into the device as "testusersimple" as described above.
2. Upon successful login you will be presented with the Held Print Jobs page:

3. Select "Print All" to release all jobs. The jobs will begin to print to the destination printer. (The "Print All" button will not appear if there are no jobs to print)
4. Once completed press the "Logout" button on the device keypad.

5.5 Scenario 4: Scanning and faxing

Canon devices can also scan documents and send them by email. If a phone line is attached, they can send faxes. You can enable tracking scanning and faxing. Users can be prevented from scanning or faxing when they are out of credit.

To enable tracking of scans and faxes:

1. In PaperCut, select the "Devices" tab.
2. Select the MFD device.
3. Under "Device function" tick "Track & control scanning" and tick "Track & control faxes".
4. Select the charging type "advanced" in both cases and set some numbers for page costs and thresholds. The cost after the threshold should be lower than the standard cost as it represents a volume discount. As an example, the screen shot below shows that the first page of a fax is charged at $0.20 and any subsequent page at $0.10.
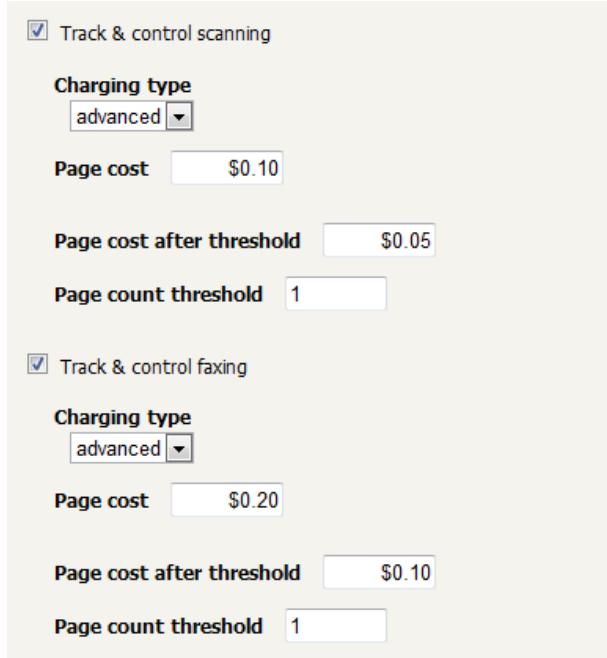
At the photocopier, log in and scan a few documents and send a few faxes. At the end, make sure to press the "Logout" button on the device's keypad.

In the PaperCut administration interface verify that the scan and fax activities were recorded and the user's account was deducted. This can be done as follows:

1. Log in to the PaperCut administration interface.
2. Select the device from the "Devices" tab.
3. Select the "Job Log" tab. This will list all recent activity on the copier, including copying, scanning and faxing. The jobs just performed as the test user should be listed. Verify the details of the jobs that were just performed.

Usage Date ▼	User	Charged To	Pages	Cost	Document Name	Attrib
Dec 9, 2009 11:45:23 AM	testusersimple	testusersimple	2	$0.30	[fax]	
Dec 9, 2009 11:44:35 AM	testusersimple	testusersimple	5	$0.30	[scanning]	

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 activity for the user.
6. Select the "Transaction History" tab and verify that the cost of the scans and faxes was deducted from the user's account.

Transaction date ▼	Transacted by	Amount	Balance after
Dec 9, 2009 11:45:23 AM	[system]	-$0.30	$4.40
Dec 9, 2009 11:44:35 AM	[system]	-$0.30	$4.70

6 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 those default settings. All the following settings are available via the device's 'Summary' tab in the PaperCut administration interface.

6.1 Device Function

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

Each device function is discussed in the following table.

Device Function	Description
Track & control copying	The device will track walk-up off-the-glass copying.
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 release station	The device will act as a print release station.

6.2 Authentication Methods

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

The available authentication methods can be modified in the 'External Device Settings -> Authentication methods' section.

Authentication methods

☑ Username and password

☑ Identity number

    ☑ Require PIN

    ☐ Mask identity number

☐ Swipe card

☐ Anonymous (No login required)

Authentication methods available for a device

Not all authentication methods are supported on all devices. A grayed-out option indicates that the option is not supported on this device.

Each authentication method is discussed in the following table.

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 with their identity number. Identity numbers are convenient when usernames are long or cumbersome to enter. For example, rather than entering a username like 'john.smith.001', it may be more convenient to enter an employee ID of '1234'. See the PaperCut user manual for information about user identity numbers, including importing identity numbers from an external source.
Identity number -> Require PIN	When a user logs in with their identity number, they must also provide their associated PIN. This provides additional security for identity number logins.
Anonymous (No login required)	Specifies that this device should always automatically log in as the specified user. This option overrides all other authentication methods

Description of authentication methods

7 Advanced Configuration

7.1 Config Editor

The common configuration options for a device in PaperCut are available on the device's "Summary" tab, and are discussed in more detail in 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-msg.welcome	Optionally customize the message displayed on the welcome page e.g. PaperCut Software\nPlease swipe your card to login.
	Specifying "\n" starts text on a new line. Be aware of the limited screen space available on MFDs.
	Default: DEFAULT
ext-device.block-release-on-error.snmp-error-list	Defines the error types that will block the release of jobs from the MFD Print Release. Valid values:
	• DEFAULT—includes noPaper, doorOpen, jammed,offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull
	• A comma-separated list of error types. Valid error types include lowPaper, noPaper, lowToner, noToner, doorOpen, jammed, offline, serviceRequested, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputNearFull, outputFull, inputTrayEmpty, overduePreventMaint
ext-device.canon.accounts.initial-tab	Set to "LIST", "SEARCH" or "CODE" to make the account selection screen start on the "from List", "Search" or "by Code" tab respectively.
	If you have many shared accounts you may wish to set this to "SEARCH". An example of this is legal firms who use shared accounts for matter codes.
	Default: "LIST"
ext-device.canon.card-	Comma-separated list of card reader identification numbers composed of the vendor ID and product ID e.g. 09d8:0310.

reader-ids	See [Enable USB Input for Keyboards, Card Readers and Storage Devices](#)
ext-device.canon.email.personalized-sender	When enabled, pre-populate the email address in the device's Scan-to-Me function, as stored in the PaperCut user's details. Default: Y (Yes)
ext-device.canon.header.textcolor	See chapter [Customizing the Header Text Color](#).
ext-device.canon.limit-reference.duplex ext-device.canon.limit-reference.grayscale ext-device.canon.limit-reference.paper-size	PaperCut will deny device access to restricted users who do not have enough balance to copy. To determine if a user has enough balance to copy a reference copy is required. By default, PaperCut checks if the user has enough balance to copy one grayscale single sided Letter (North America) or A4 (worldwide) page. In some situations, it may be desirable to change the reference copy, such as when the device allows smaller page sizes like A5. Default for ext-device.canon.limit-reference.duplex: N (No) Default for ext-device.canon.limit-reference.grayscale: Y (Yes) Default for ext-device.canon.limit-reference.paper-size in North America: Letter Default for ext-device.canon.limit-reference.paper-size worldwide: A4
ext-device.canon.release.show-cost	Specify whether to show the job cost for each print job in the job release screen. Default: Y (Yes)
ext-device.canon.restricted.allow-multiple-login	Enabling this allows users to log in and charge copy jobs to a restricted account (user account or shared account) if another copy job charged to the same account is still in progress. This may cause cost overruns with users going into negative balance. Default: N (No)

ext-device.canon.swipe-to-logout	Select whether swiping a card reader when logged in to the device, logs the user out. Default: Y (Yes)
ext-device.canon.timeout. complete-scan-job.secs	**When scan tracking and fax tracking are both enabled.** Specify the number of seconds to wait for a fax job to commence after a scan job has completed. This prevents a user from being charged for the scanning component of a fax job. Default: DEFAULT (60)
ext-device.canon.timeout. session.mins	Specify the number of minutes before user session details are discarded. Session details are kept on the device for jobs completing after a user has logged out. Default: DEFAULT (1440 minutes, 24 hours) Examples: 60, 1440
ext-device.canon.message -timeout.secs	Specify the timeout period for all messages displayed on the MFD panel. Enter a negative value if you do not want messages to time out. Default: DEFAULT (10)
ext-device.card-no-converter	See [Configuring Swipe Card Readers](#).
ext-device.card-no-regex	See [Configuring Swipe Card Readers](#).
ext-device.card-self-association.use-secondary-card-number	Select whether user self-association should occupy the primary or secondary card number. This 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 setting.

ext-device.self-association-allowed-card-regex	Specify a regular expression that limits which card numbers are accepted for associating swipe cards with user accounts. See [Authentication Methods](#) for details. Defaults to ".*" (dot-star) which includes all card numbers.

7.2 Configuring Swipe Card Readers

Swipe cards contain numbers used to identify users according to the card number configured in the User Details screen under "Card/Identity" number. Some readers report information in addition to the number encoded on the card, such as checksums. PaperCut can treat these cases in three ways:

Card Number Needs No Conversion

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

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 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 in "Config editor (advanced)" which is located on the "Options" tab under "Actions". The key is called "ext-device.card-no-regex".
    - Additionally, the global setting can be overridden on a per-device basis: The key "ext-device.card-no-regex" can also be found on the "Advanced Config" tab in the device details screen. This setting will override the global setting unless the keyword "GLOBAL" is specified.
    - PaperCut developers 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 this. 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*`

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 regex's, the convertors may be defined on either a global (all devices) or a per-device basis. To set globally:

- Options -> Actions -> Config Editor
- 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**

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 logger message with conversions applied (assuming the card is unknown to the system). Try different converters and inspect the resulting numbers in the application log.

Using custom JavaScript
If the inbuilt converter functions are unable to meet 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 `[app-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`

Other advanced notes

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

7.3 Customizing the Header Logo

The embedded application displays a header logo at the top of the device screen. This header can be replaced with your own organization's logo image.

The PNG image should be 80 pixels high with the name "header.png", and placed at the following location:

`[app-path]\server\custom\web\device\canon\`

You may need to create the subdirectories if they do not already exist.

Make sure to verify the custom header logo appears correctly on the device.

Note: Some devices do not support PNG images with an alpha channel (transparency). This is a common cause of the custom image not displaying in the header. Use an image editing program to remove the alpha channel.

7.4 Customizing the Header Text Color

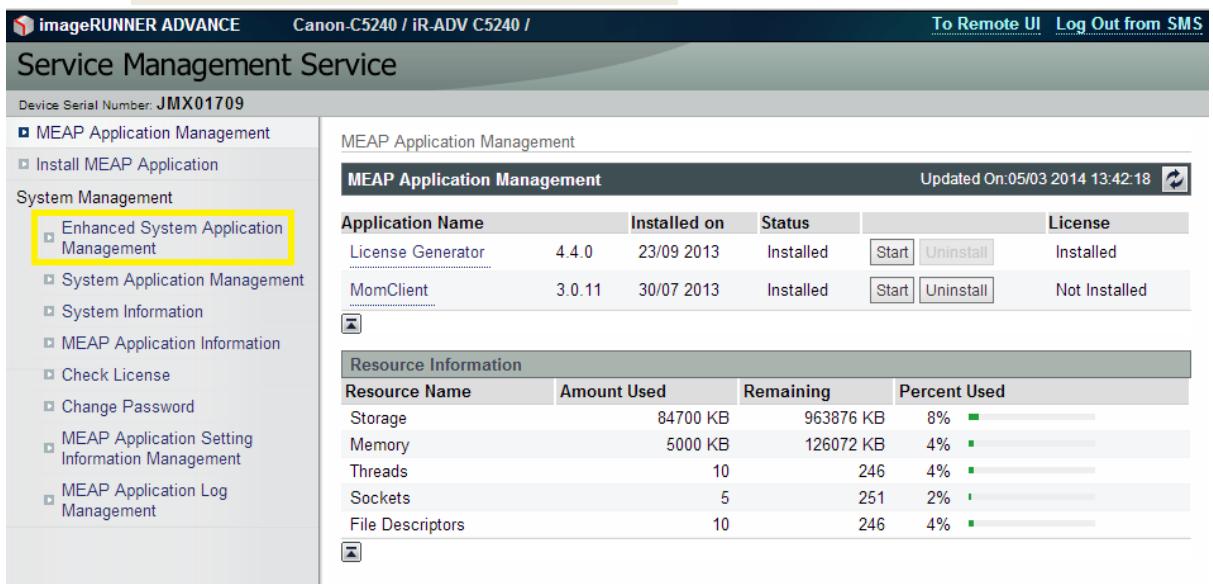The header text color can be customized via the "Advanced Config" tab in the device details screen, see Config Editor:

- ext-device.canon.header.textcolor – the text color (specify DEFAULT for the default setting of white)

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

8 Uninstalling

To uninstall the "PaperCut" Login Service:

1. Log on to the device's administration page at `https://<device-ip-address>:8443/sms/`.

2. Select the **Enhanced System Application Management** option on the left-hand side.

3. The "PaperCut" login service needs to be disabled before it can be removed from the device.

   Switch to the "Default Authentication" login service by selecting the associated **SWITCH** button.

4. Restart the device and log back into the device administration page as per steps 1 and 2 above.

5. Press the "PaperCut" login service's associated **Uninstall** button.

6. You will be asked to confirm. Press the **Yes** button.

9 Known Limitations

This section lists known limitations with the Canon MEAP implementation.

9.1 Controlling USB jobs

Note: *This section refers to the supported devices listed in*
http://www.papercut.com/tour/embedded/canon#supported.

Printing from USB media and scanning to USB media are correctly tracked within PaperCut. However, these jobs cannot be controlled; meaning the jobs cannot be stopped from occurring. Printing and scanning via USB media can be disabled on the device if required. See Managing USB Storage Media.

9.2 Zero-stop

Ideally, PaperCut can control exactly how many pages a user can copy, and always prevent the user from overdrawing their account. Canon devices offer the ability to limit page counts, but copying does not necessarily stop immediately when those limits are reached. This delay means that users may overrun their account below zero, by one or more pages.

9.3 Devices with limited/no Fax Logging and Tracking

Note: *This section refers to the supported devices listed in*
http://www.papercut.com/tour/embedded/canon#supported.

These models do not carry the mechanisms needed by PaperCut to both log and control Faxing.

On these devices, PaperCut may not be able to log faxing activity, and will not be able to prevent users with insufficient funds from faxing. In addition, faxing on these devices might be logged as a scan job (if the administrator has enabled Scan Tracking on that device in PaperCut).

9.4 Devices with limited/no Box Printing Tracking

Note: *This section refers to the supported devices listed in*
http://www.papercut.com/tour/embedded/canon#supported.

Box Printing refers to print jobs that are initiated from the device itself.
Eg. Documents stored on a local mailbox inside the MFD, network share or USB media etc.
On some devices, these actions are accessible through the 'Access Stored Files' menu option.
These models do not carry the mechanisms needed by PaperCut to both log and control such print jobs.

On these devices, PaperCut will not be able to log such print jobs, and will not be able to prevent attempts by users with insufficient funds to print such documents.

9.5 Color Restrictions

Color restrictions are available when the Access Management System (AMS) is installed and enabled on a Canon device. Devices without AMS installed and enabled are unable to perform color restrictions.

9.6 Waking up the touchscreen

A device's touchscreen is turned off when in energy saving mode. Card swiping an attached card reader logs in to the device, but not all devices are capable of 'waking up' the touchscreen without the user pressing the 'Energy Saver' hard key.

9.7 White screen displayed after logging in with an identity number

If you have selected **Identity number** as the **Authentication method** on the **Device Details** page in the PaperCut MF Admin interface, some devices might display a white screen after logging in with the identity number.

If you experience this issue:

1. On the MFD, select **Settings > Registration > User Management > Department ID Management > Settings**.
2. Clear the **Enable Department ID Management** option.

10 FAQ & Troubleshooting

What is the IP address of my PaperCut Server?

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

The embedded application shows "Device Setup: failed to connect to …"?

This indicates that the embedded application is unable to connect to the PaperCut server over the network. The embedded application will continually try to connect to the server, so if there is a temporary network outage it will start working once the connection is available again.

Common causes of this problem are:

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

Jobs performed on the MFD are not tracked in PaperCut?

Have you enabled job logging? See Enable Job logging.

Why would a card reader not work?

Not all card readers are supported. See Enable USB Input for Card Readers and Card Reader support.

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

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