PaperCut Toshiba LeSF Embedded Manual

Contents

1 Overview 3
1.1 Consistency 3
1.2 Integration 3
1.3 Rate of development 3
1.4 Vendor Neutral 3
1.5 Security 4
2 Installation 5
2.1 Requirements 5
2.1.1 Supported Devices 5
2.2 Setup Procedure 5
2.2.1 PaperCut Settings 5
2.2.2 Locating the Embedded Application File 5
2.2.3 Installing the Embedded Application 5
2.2.4 Setting Login Timeout 7
2.2.5 Disabling “Held Jobs” 7
2.2.6 Security Lock-Down 8
2.2.7 Additional Network Security (optional) 8
2.3 Upgrading to a newer version 9
3 Post-install testing 10
3.1 Test Preparation 10
3.2 Scenario 1: Standard copying 11
3.3 Scenario 2: Copying with account selection 12
3.4 Scenario 3: Print release 13
3.5 Scenario 4: Scanning 15
4 Configuration 17
4.1 Device Function 17
4.2 Authentication Methods 17
4.3 Shared Account Selection 18
4.4 Customizing Text and Messages 18
4.5 Tracking Jobs from Non-Standard Applications 19
4.6 Automatic Sign-On to Applications 20
4.7 Configuring Application Access Controls with PaperCut Security Templates 20
5 Advanced Configuration 21

5.1 Config Editor 21
5.1 Customizing the Header Logos and Colors 24
5.1.1 Customized Logos 24
5.1.2 Custom Header Color 25
5.2 Configuring Swipe Card Readers 26
5.2.1 Card Number Needs No Conversion 26
5.2.2 Regular Expression Filters 26
5.2.3 Card Number Format Converters 26
5.2.4 Standard Converters 27
5.2.5 Using custom JavaScript 27
5.2.6 Other advanced notes 28
6 Known Limitations and Security 29
6.1 Known Limitations 29
6.2 Security concerns 29
7 FAQ & Troubleshooting 30
A. Appendix: Supported Authentication Card Readers 31
B. Appendix: Screenshots for User Information Sheets 32

This manual covers the Toshiba LeSF embedded MFD setup. For general PaperCut MF documentation, please see the PaperCut MF manual.

1 Overview

Note: Toshiba is a Trademark of Toshiba, USA and LeSF is a trademark of Lexmark USA. PaperCut is solely responsible for the contents of this publication and the performance of PaperCut's products.

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 function access via user authentication (including integration with single sign-on environments)
- Monitoring and control of photocopying, scanning, faxing and USB printing (silent tracking, quotas, charging, allocation and logging)
- Allocation of copying, scanning, and faxing to accounts/departments/cost-centers/projects
- 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)
- Group based access control: Limit access to color copying or to the device as a whole to selected user groups.

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 and users have to learn only one system.

1.2 Integration

PaperCut is a single integrated solution where print, internet and copier control are all managed in 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 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 operating systems including Windows, Linux, Mac and Novell.

1.5 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 cannot be satisfied, any deficiencies are fully disclosed.

2 Installation

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

2.1 Requirements

Ensure that the following requirements are satisfied before getting started:

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

2.1.1 Supported Devices

The following devices are compatible with the PaperCut solution

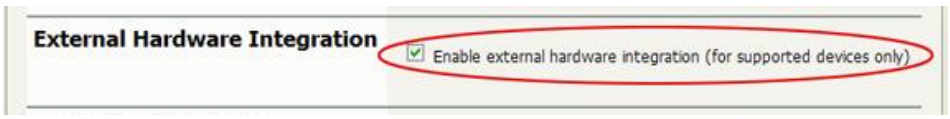
- TOSHIBA e-STUDIO430S
- TOSHIBA e-STUDIO530S

Please ask your local Toshiba supplier to make sure your devices are running an up to date firmware version.

2.2 Setup Procedure

2.2.1 PaperCut Settings

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



3. Click 'Apply'.

2.2.2 Locating the Embedded Application File

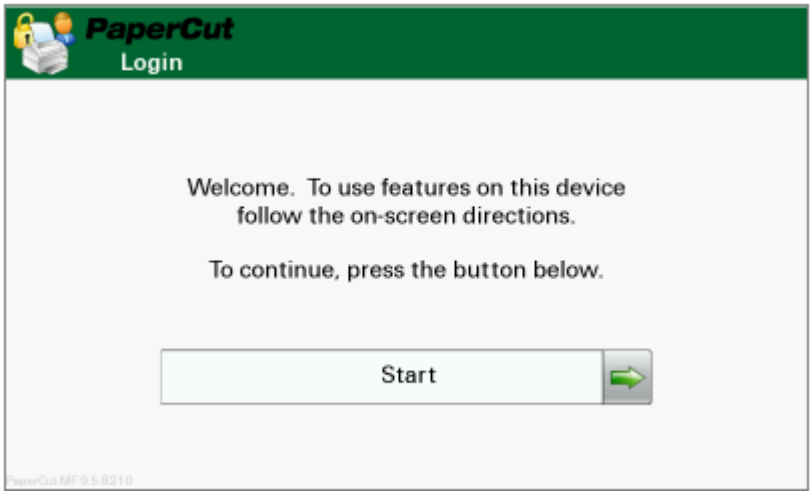
The files are located under your PaperCut installation directory on the server, in the subdirectory `[app-path]/providers/hardware/Toshiba`.

2.2.3 Installing the Embedded Application

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

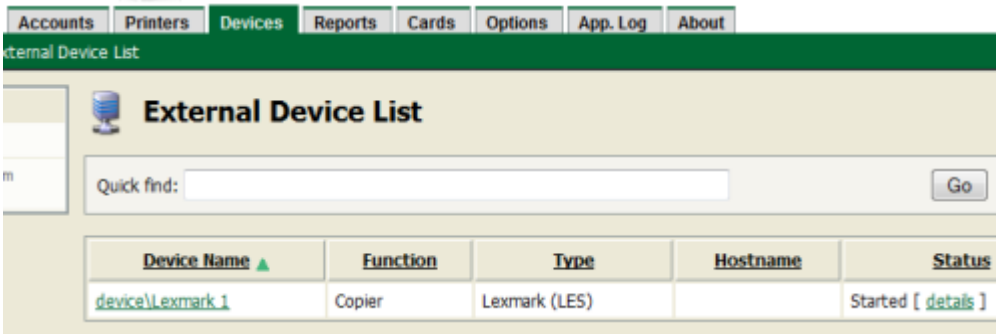
To install the application, perform the following steps:

1. Turn on the Toshiba device.
2. On a computer, open your web browser
3. Enter the URL of the Toshiba device. E.g. http://Toshiba-device-ip/
4. Select the “Settings” menu option from the left (also called “Configuration” on older devices).
5. Select “Embedded Solutions”. On newer devices this is called “Device Solutions” instead.
    a. If your solution page is called “Device Solutions” select “Solutions (LeSF)” on it. **Do not** select “Additional Solutions”.
6. Click the “Install” button.
7. Click the “Browse …” button and select the appropriate application FLS file.
8. Click “Start Install”.
9. A confirmation message will appear. Click “Return” to return to the Embedded Solutions list.
10. The list should now show an item labeled “PaperCut” and the “State” column should show “Running”.
11. Click the “PaperCut” item and click on the “Configure” button that appears.
12. Enter a unique device name such as “Toshiba 1” or “Library Copier” that will later appear in PaperCut’s list of devices.
13. Enter the PaperCut server’s hostname or IP address under “Server Hostname”. You may need to use the IP address if DNS is unable to resolve the server name correctly.
14. Leave all other settings at their defaults and click “Apply”.
15. The PaperCut login screen will now be displayed on the device.



16. The Toshiba device will appear in the PaperCut administration interface under the “Devices” tab with the name you provided in the steps above. The cost settings of

the “[Template Printer]” on the “Printers” tab will be applied to this device.



17. The embedded application is now successfully installed. To use the photocopier, the users must login to the application, and any copying they perform will be logged in PaperCut.

2.2.4 Setting Login Timeout

After logging into the device it will show the “home screen” that presents the functions available such as copying, scanning, and faxing. This screen will also show after completion of each function. By default, Toshiba devices will return to the login screen after a timeout of typically 5 seconds, requiring the user to go through the login procedure again. We recommend setting this timeout to 10 seconds, keeping in mind the following:

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

To set the timeout to a different value:

- Access the Toshiba web admin interface under http://Toshiba-device-ip/
- Select “Settings” on the left-hand menu bar
- Select “Security” under “Other Settings”
- Select “Miscellaneous Security Settings”
- Select “Login Restrictions”
- Enter a new value such as “10” under “Panel Login Timeout” and click “Submit”.

2.2.5 Disabling “Held Jobs”

Toshiba devices provide a feature called “Held Jobs” which conflicts with PaperCut’s hold/release queues. “Held Jobs” should be deactivated in order to avoid confusion with PaperCut’s print release functions.

- Access the Toshiba web admin interface under http://Toshiba-device-ip/
- Select “Settings” on the left-hand menu bar
- Select “General Settings”
- Select “Home Screen Customization”
- Uncheck “Search Held Jobs” and “Held Jobs” and click “Submit”

2.2.6 Security Lock-Down

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

- Access the Toshiba web admin interface under http://Toshiba-device-ip/
- Select “Settings” on the left-hand menu bar
- Select “Security” under “Other Settings”
- Select “Edit Security Setups”
- Select “Password”
- Select “Add a Password”
- Enter “Admin” for the “Setup Name” and enter a password twice, **also check the “Admin Password” checkbox**, then click “Submit”
- Select “Return to Edit Security Setups”
- Select “Security Templates”
- Select “Add a Security Template”
- Enter “Admin” for the “Security Template Name”, choose “Admin” from the “Authentication Setup”, and click “Save Template”
- Click “Return to Edit Security Setups”
- Select “Access Controls”
- Set **all options** to “Admin”, or if “Admin” is not available, to “Disabled”. Exceptions:
    - Set “Operator Panel Lock” to “Disabled”
    - Set “Copy Function” to “No Security”
    - Set “Use Profiles” to “No Security”
- This will deny users access to any functions other than copying and print release. You may revisit this setup later on a case by case basis and re-enable other functions such as e-mail or fax. If you are uncertain of how to set a particular feature you should deny access by setting it to “Admin” or “Disabled”.
- Click “Submit”

2.2.7 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.

2.3 Upgrading to a newer version

The procedure for upgrading an existing embedded application to a newer version is similar to the initial installation (see Section 2). Please note that only the device-level installation needs to be performed, and you shouldn't have to perform any additional configuration within the PaperCut administrator interface.

After upgrading, it's worth verifying that the Embedded Application's version number matches the expected value.

3 Post-install testing

After completing installation and basic configuration testing the common usage scenarios is recommended. 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.

3.1 Test Preparation

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

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

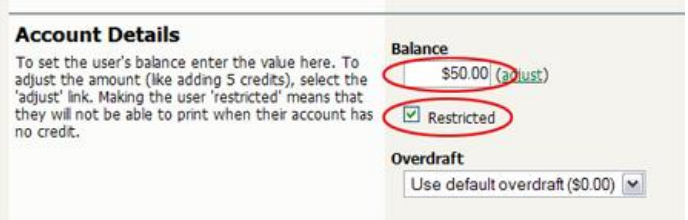
To setup these users in PaperCut:

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

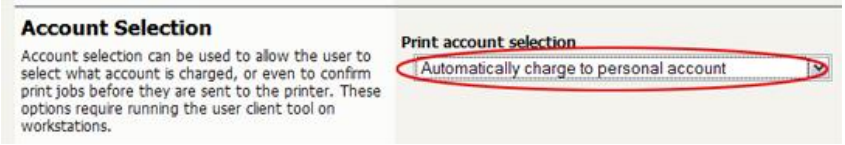
The next step is to configure these users.

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 that the account is set to "Restricted".



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

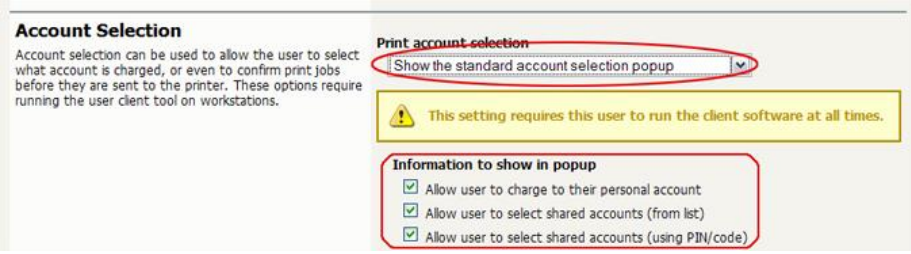


5. Press the "OK" button to save.

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 of the account selection options.



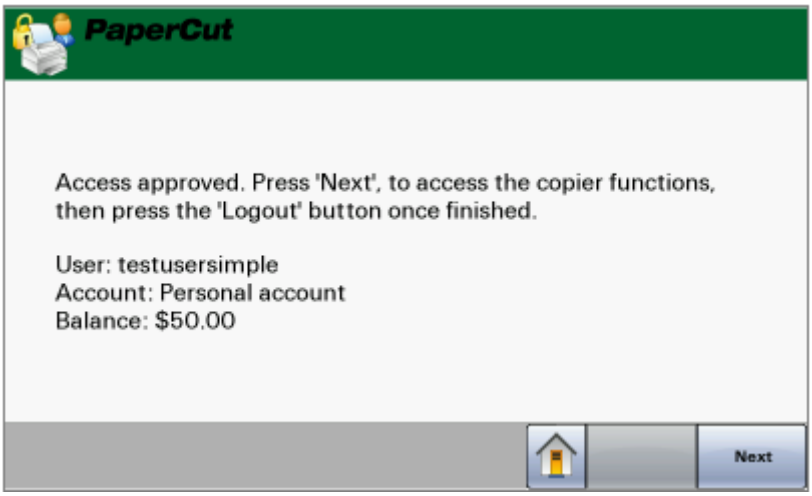
4. Click the “OK” button to save.

3.2 Scenario 1: Standard copying

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

At the photocopier device:

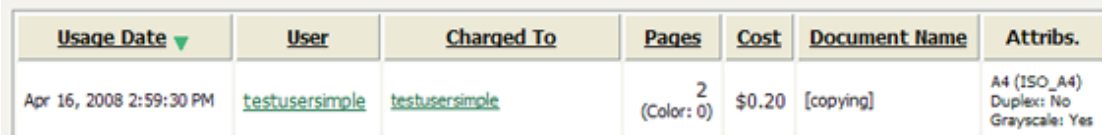
1. At the “Login” screen, press “Start”.
2. Enter the ‘testusersimple’ username and password.
3. The device will show the home screen with a choice of functions including “Copy”.
4. Press the “Copy” button and perform a copy as normal.



5. Once copying is completed the device will return to the home screen.
6. Press the “Logout” button.

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

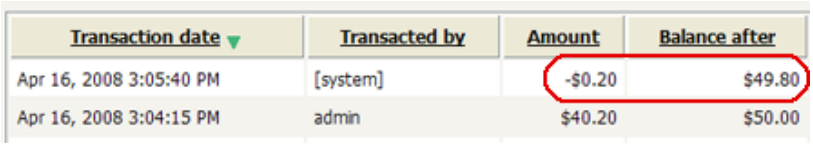
1. Log in to PaperCut.
2. Select the device from the “Devices” tab.
3. Select the “Job Log” tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed. Verify the details of the copy job that was just performed.



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

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

5. Select the “Job Log” tab to display all print/copy activity for the user.
6. Select the “Transaction History” tab and verify that the cost of the photocopying was deducted from the user’s account.



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

3.3 Scenario 2: Copying with account selection

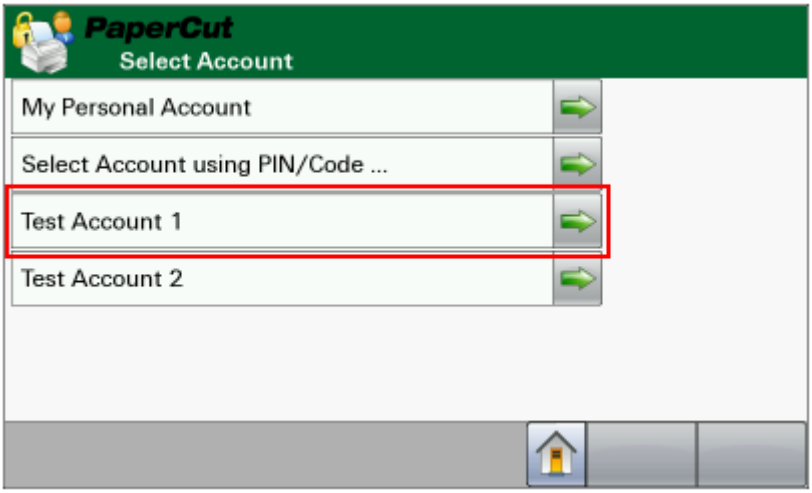
Copying can be allocated to “shared accounts” that represent departments, projects or cost centers. This is commonly used by staff in academic organizations to allocate printing to departments.

First some test accounts should be created:

1. Log in to PaperCut, select the “Accounts” tab.
2. Select the “Create a new account…” action link on the left.
3. Enter the account name “Test Account 1”.
4. Click “Apply”.
5. Select the “Security” tab and allow all users to access that account by adding the “[All Users]” group.
6. Press “OK”.
7. Repeat this process to create some more accounts.

At the photocopier device:

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



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

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

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

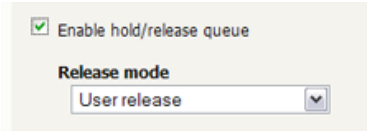
3.4 Scenario 3: Print release

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

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

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

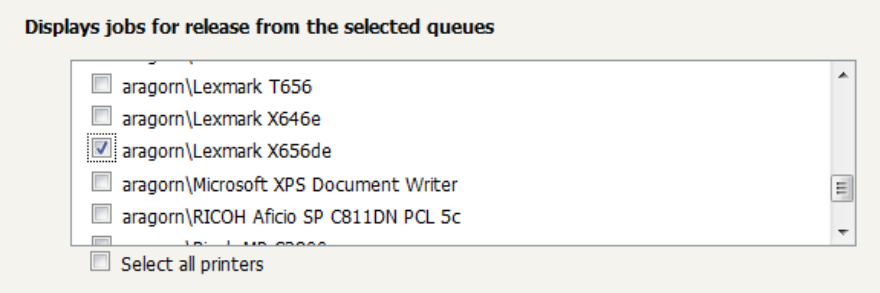
1. In PaperCut, select the “Printers” tab.
2. Select the print queue (not the ‘device’) for the Toshiba MFD that will be used for testing.
3. Enable the “Hold/release queue” option.



4. Click OK or 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 Toshiba MFD’s device.
3. Under “Device functions” tick “Enable release station”.
4. Select the print queue that was enabled for hold/release above. The Toshiba device will allow jobs on the selected queues to be released.



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 photocopier device:

10. At the “Login” screen, press “Start”.
11. Enter the ‘testusersimple’ username and password.
12. The device will show the home screen with a choice of functions including “Print Release”.
13. Press the “Print Release” button.
14. The list of held print jobs is displayed.

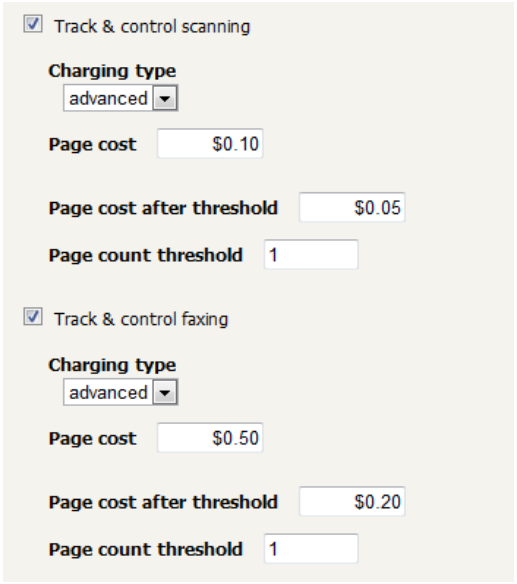
15. Select the job to release by pressing the arrow next to the job.
16. Confirm the release of the print job by pressing the “Print Job” button.
17. The job will then print.
18. Try cancelling a job by selecting it and then pressing the “Cancel Job” button.
19. The job will be cancelled and will not print.

3.5 Scenario 4: Scanning

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

To enable tracking of scans and faxes:

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



At the device, log in as ‘testusersimple’ and proceed to do faxing and scanning as usual. Both Scan-to-Email and Scan-to-FTP are supported. Please consult your device manual for details of these operations.

Back in the PaperCut administrator web interface, the job log for the device will show the scan and fax jobs with their respective destinations:

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

Note on sending to multiple destinations:

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

Note on point-of-charging for faxes: Fax jobs are scanned and then stored by the device for later (asynchronous) faxing. While fax jobs are pending, the red “Cancel Jobs” button will be

displayed on the device's home screen and can be pressed to inspect the pending jobs and cancel them individually. Note that charging of faxes is delayed until sending over the telephone line has succeeded.

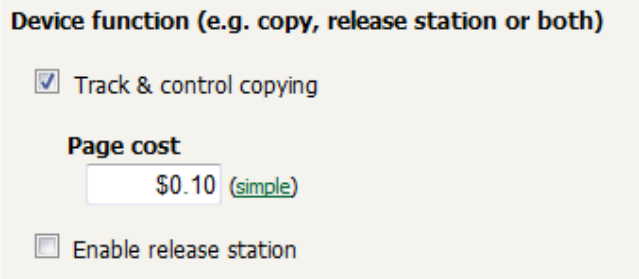
- This has the benefit that canceled fax jobs will not be charged.
- While restricted users' account balance is checked for sufficient credit during the scan process of a fax job, users may be able to deplete their credit before the fax has completed sending and delayed charging of faxes may result in users overrunning their account balance.

4 Configuration

After completing the Installation section and registering the device with PaperCut, it will be configured with default settings that are suitable for most environments. This section covers changes to the default settings. All of the following settings are available via the device's 'Summary' tab in the PaperCut administration interface.

4.1 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.



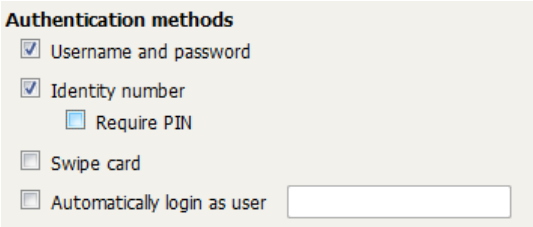
Each device function is discussed in the following table.

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

4.2 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 (usually backed by a directory service such as Active Directory or LDAP).

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



Authentication methods available for a 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.
Swipe card	The user may log in by swiping 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. Please see Appendix 0 below for a list of supported card readers.
Swipe card -> Require PIN	When a user logs in by swiping a card, they must also provide their associated PIN. This provides additional security for swipe card logins.
Swipe card -> Enable self-association with existing user accounts	Available Q1 2010: Users can swipe cards previously not used or registered at the device with PaperCut and will be prompted for their username and password. The swipe card can then be used at subsequent logins. See chapter 5.1 for advanced configuration of this function.
Automatically login as user	Specifies that this device should always automatically log in as the given user. This option overrides all other authentication methods

4.3 Shared Account Selection

Shared account selection options at the MFD mirror the options presented in the PaperCut client print popup. The options available include:

- Select from a list of shared accounts
- Search for shared accounts by keyword
- Select account using PIN/Code

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" and/or "Select using PIN/Code" are controlled at the user level via the *User Details* page. The "Security" tab on each account controls account security and access.

Note: The search option will only appear if the account list is long. Short lists of only a few accounts will not list a search option.

4.4 Customizing Text and Messages

PaperCut allows some text that appears in the device to be customized. Custom text might include instructions or terminology that is more appropriate for the site. An example of text that is customizable is the "Welcome text" that displays before the user logs in to the device.

The text can be customized by editing the device configuration from the PaperCut administration interface. For more details see the following Advanced Configuration section.

4.5 Tracking Jobs from Non-Standard Applications

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

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

If “automatically charge to personal account” or “automatically charge to single shared account” are configured for a PaperCut user, non-standard application usage will be automatically charged to the user’s personal account or pre-defined shared account respectively. For any other account selection option, the default behavior is to charge jobs from non-standard applications to the user’s personal account.

Jobs from non-standard applications are not subject to credit limits of restricted personal or shared accounts, i.e. users can overrun credit limits by producing jobs through non-standard applications. In environments where enforcing credit limits is desired, it is recommended to disable non-standard applications by removing them from the home screen via the device’s web configuration.

Charging can be configured to display an account selection dialog and charge non-standard application jobs to the selected account instead. Two options are available for non-standard application account selection, each with different limitations:

- Account Selection from Home Screen can be shown when the user selects presses the non-standard application at the home screen. This is similar to account selection when pressing the buttons for the standard applications, but with the following limitations:
    - The non-standard application needs an “Access Control” in the “Security” menu of the device’s web configuration.
    - Account selection will only be shown once during the session for the selected application and all other non-standard applications. This means that subsequent re-selection of the application from the home screen will not result in the account selection being shown again, nor would selecting another non-standard application. As a consequence, all jobs from non-standard applications will be charged to the selected account until logout.
    - Automatic Sign-On to Applications (see section 4.6) cannot be activated at the same time.

  To enable Account Selection from Home Screen, configure access control for each non-standard application with a PaperCut security template (see section 4.7). Make sure to configure a different security template (e.g. PaperCut 1, PaperCut 2, etc.) for each application.
- Account Selection at Login can be shown after the user has successfully entered their credentials or swiped their card, with the following limitations:
    - The account selected at login will be used to charge all jobs during the session and no further account selection will be shown until logout. This applies to standard as well as non-standard applications.
    - If print release is enabled, a print release screen will be shown as part of the workflow before account selection. This is to prevent account selection just to

release print jobs, however at least one additional screen press is required to transition from print release to account selection.

To enable Account Selection at Login, set the advanced configuration property “ext-device.toshiba.login.account-selection” to “Y” (see section 5.1).

4.6 Automatic Sign-On to Applications

Copier applications like “Scan to Network” and “Forms and Favorites” require the user to sign-on to the application using username and password even while successfully logged into PaperCut. The application will use this second set of credentials to authorize against a network share to deposit scanned documents (Scan to Network) or retrieve documents to print (Forms and Favorites).

Other 3rd party applications (e.g. document workflow applications) require just the username of the authenticated user in order to direct scanned documents to the correct destination.

PaperCut can be configured to automatically pass the user’s PaperCut credentials to the application requiring sign-on, subject to the following limitations:

- PaperCut can only pass credentials to one application. E.g. if both “Scan to Network” and “Forms and Favorites” are present on the copier, one of them has to be selected for automatic sign-on, all other applications require manual sign-on as before.
- In case the application needs both username and password for its functionality, the user has to log in with username and password. If the application only needs the username, any login method will work.
- Application sign-on is incompatible with Account Selection from Home Screen for non-standard applications as described in section 4.5. If account selection for non-standard applications is required with application sign-on, Account Selection at Login has to be enabled.

To enable automatic sign-on to an application, configure the application’s access control with a PaperCut security template (see section 4.7). Next, change the advanced configuration property “ext-device.toshiba.app-sign-on” from “OFF” to the appropriate access control identifier:

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

- For access control identifiers of other applications please contact PaperCut support.
- Some applications can be configured to use the all-purpose numeric access controls “Solution 1” to “Solution 10”. In this case the access control identifier is the number 54 plus the solution number added, e.g. for “Solution 5” the identifier is “59”.

4.7 Configuring Application Access Controls with PaperCut Security Templates

Account selection for non-standard applications (section 4.5) and application sign-on (section 4.6) may require configuring access control for one or more device applications with a PaperCut security template. To do so:

- Access the device’s web interface at http://<device-ip>
- Navigate to Settings > Security > Security Setup

- Under “Advanced Security Setup” click “Security Template” in “Step 2”.
- Click “Add a Security Template”.
- In “Security Template Name” enter “PaperCut 1”.
- From the “Authentication Setup” drop-down list, select “PaperCut Authentication Module 1”.
- Click the “Add Authorization” button and wait for the page to reappear.
- From the “Authorization Setup” drop-down list, again select “PaperCut Authentication Module 1”.
- Click “Save Template”.
- Click “Return to Security Setup” to return to the main security screen.
- Click “Access Controls” in “Step 3”.
- Find the application you would like to configure an access control for in the list.
    - If the list is presented as a list of small yellow folders, it can most likely be found the “Device Solutions” folder.
    - Depending on the device application and its configuration, the corresponding access control may be one of the generic “Solution 1” to “Solution 10” access controls.
- From the corresponding drop-down list, choose “PaperCut 1”.
- Click “Submit”.

Repeat this process for every device application that you would like to configure an access control for as per instructions from the previous sections, increasing the number for the security template every time. E.g. for the second application, create a security template named “PaperCut 2” with “PaperCut Authentication Module 2”, then “PaperCut 3” with “PaperCut Authentication Module 3” etc. A maximum of 5 security templates can be created this way and assigned to a maximum of 5 access controls.

5 Advanced Configuration

5.1 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 uncommon configuration options which are available via the ‘Advanced Config’ tab in the devices details screen.

Config name	Description
ext-device-msg.welcome	The text displayed on the welcome screen. This text can be used to provide specific information about logging in to the device. Use “\n” to create a new line. Default: DEFAULT (uses the default application text).
ext-device-msg.card-association	Message to display when users are requested to associate their swipe card with an existing user account. See chapter 4.2 for details. Specify “DEFAULT” for the default text.
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 chapter 4.2 for details. Please contact PaperCut support for help with regular expressions. Defaults to ".*" (dot-star) which includes all card numbers.
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.toshiba.hold-copies	If set to "Y", will perform copies by scanning all pages first and then starting printing. If set to "N" printing starts after the first page has been scanned. This option is ignored on devices without a hard disk where printing will always start after the first page. Set to "DEFAULT" for "Y" on devices with a hard disk and "N" on devices without a hard disk.
ext-device.toshiba.header.color	See chapter 0.
ext-device.toshiba.header.textcolor	See chapter 0.
ext-device.release-all-on-login	Set to yes to have a user's documents that are pending release automatically released on login. The user will not have to select the "Print Release" function on the device. This is particularly convenient in conjunction with swipe card authentication, allowing print release without any screen interaction.
ext-device.toshiba.release.show-busy	Set to yes to show a warning message when users are releasing documents while the device is still busy printing or copying.
ext-device.toshiba.release.show-busy.job-timeout	When the ext-device.toshiba.release.show-busy option is enabled then jobs that have been paused (paper jam, out of paper) for this time are considered not to be keeping the printer busy.
ext-device-msg.busy-on-release	Message to display when the ext-device.toshiba.release.show-busy.job-timeout option is enabled. Specify "DEFAULT" for the

	default text.
ext-device.inactivity-timeout-secs	Defines the time period for which a user is allowed to wait between key presses before they are automatically logged out. Default: 60
ext-device.card-no-regex	See chapter 0.
ext-device.toshiba.email.personalized-sender	If set to “Y” and the email field of the user logged onto the Toshiba device has been populated in PaperCut, will set this email address as the “From” field in the scan-to-email function. Depending on device model and firmware, “Track and Control Scanning” may have to be enabled.
ext-device.toshiba.email.personalized-destination	If set to “Y”, “Track and Control Scanning” is enabled and the email field of the user logged into the Toshiba device has been populated in PaperCut, will set this email address as the “To” field in the scan-to-email function.
ext-device.toshiba.email.locked-destination	If set to “Y” users cannot change the “To” field in the scan-to-email function. Only use this in conjunction with setting “personalized-destination” to “Y”: Users will only be able to send email to themselves.
ext-device.toshiba.show-account-confirmation	Default: “Y”. If set to “N” the message confirming the account selection will be skipped resulting in a more fluent workflow. In particular, if account selection is pre-set for all users to their personal or a single shared account and the account is unrestricted the confirmation message is of limited value and should be skipped.
ext-device.toshiba.paper-size.default	Default “A4”/”LETTER” depending on country. Paper size that will be recorded for a copy job when “Auto Size Match” paper size is selected.
ext-device.toshiba.login.account-selection	Default: “N”. If set to “Y”, will display account selection and/or print release during the login process. See section 4.5 for details.
ext-device.toshiba.app-sign-on	Default: “OFF”. Enter an applications’ access control identifier here for automatically signing on to that application on with PaperCut credentials. See section 4.6 for details.

5.1 Customizing the Header Logos and Colors

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

5.1.1 Customized Logos

The embedded application header has two header logos (as shown below). These logos can be replaced with your organization's logo.

This shows the two logos outlined in red. The images are must be saved as GIF files with the following filenames and sizes:

- Icon logo: `icon-logo.gif` – 64 x 64 pixels
- Text logo: `text-logo.gif` – 150 x 38 pixels

These images should be saved on the PaperCut application server in the PaperCut application directory under the subdirectory `server\custom\web\device\Toshiba`. Create the subdirectory if necessary. The embedded application will fetch the images from the server to display them on the device screen.

Minor deviations from the recommended horizontal pixel size are possible for the text logo (wider or narrower). Verify the correct layout on the device screen after producing the image.

5.1.2 Custom Header Color

The header colors are defined in the “Advanced Config” in the devices details screen, see chapter 5.1. The options to change are:

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

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

5.2 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:

5.2.1 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`.

5.2.2 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 in the "Config editor (advanced)" which you will find on the Options tab under Actions. The key is called "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 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. Please contact PaperCut support.
    - 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*`

5.2.3 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 either globally (for all devices) or on 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**

5.2.4 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 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.

5.2.5 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`

5.2.6 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 plugin architecture that the PaperCut Software development team uses to implement these advanced converters. Please contact support to discuss development options and costs.

6 Known Limitations and Security

6.1 Known Limitations

On all devices:

- When using the “Auto Match” paper size setting, “Customer Job” mode, separator sheets or booklet printing, the cost of a job cannot be estimated accurately prior to printing. For restricted users, this may result in the job starting to print and getting stopped before it is complete. It may also result in an account overdraft of a few pages.

The following limitations may exist on some Toshiba devices:

- Depending on firmware, copy jobs with an output paper size selection of “Auto Size Match” may not perform zero-stop correctly when the output paper size is not Letter (US/Canada) or A4 (other countries).
  Inquire with PaperCut support or Toshiba whether your devices’ firmware supports “Auto Size Match” correctly. If not, this means that
  - For copy jobs with output paper sizes with a cost lower than the cost of A4/Letter the copy job may be denied with a reason of insufficient credit even when sufficient credit is available.
  - For copy jobs with output paper sizes with a cost higher than the cost of A4/Letter the copy job may result in an account overrun.

6.2 Security concerns

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

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

7 FAQ & Troubleshooting

What is the IP address of my PaperCut Server?

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

The embedded application shows "Device Setup: Connecting to server …'?

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

Common causes of this problem are:

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

I see an error on the Toshiba LCD screen?

This may indicate a configuration issue, or maybe a software bug. Re-check your settings and restart the MFD (i.e. power-off and power-on the copier). If problems continue, contact PaperCut 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.

A. Appendix: Supported Authentication Card Readers

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

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

Other keyboard emulating USB card readers may work, but should be tested prior to deployment.

Supporting Card Reader authentication is as easy as:

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

B. Appendix: Screenshots for User Information Sheets

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