PaperCut Lexmark Embedded Touchscreen Manual

Contents

This manual covers the Lexmark embedded touchscreen printer setup. For general PaperCut MF documentation, please see the PaperCut MF manual.

1 Overview

Note: Lexmark and LeSF are Trademarks of Lexmark, USA. PaperCut is solely responsible for the contents of this publication and the performance of the PaperCut's products.

This manual provides an overview of the installation, configuration and operation of PaperCut's embedded software solutions. Today's devices are smarter – they have touch screens and offer the ability to run applications directly on the device. The goal of PaperCut Software's embedded solution is to leverage these smart devices and to rich application features in the print control area. These include:

- Secure function access via user authentication (including integration with single sign-on environments)
- Release jobs from a hold/release queue (Secure & Find Me Printing)
- Group based access control

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 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 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 the installation of the PaperCut embedded application for compatible Lexmark devices. The embedded application will serve as a release station for network prints (for information on just tracking network printing see the PaperCut user manual).

2.1 Requirements

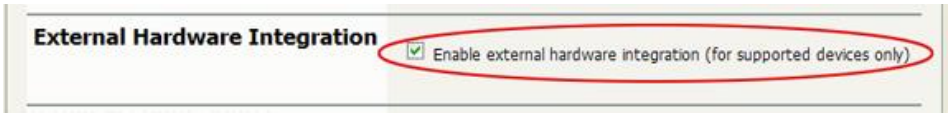
Ensure that the following points are checked off before getting started:

- 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 Lexmark device supports LeSF version 2.1 or later. The Lexmark Embedded Touch Screen Printer solution currently only supports the Lexmark model T656dne.
- 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 Lexmark device is connected to the network.

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 the option 'Enable external hardware integration' is enabled.



3. Press 'Apply'.

2.2.2 Locate the application flash file

The PaperCut Lexmark Embedded application for touch screen printers is contained in a file named "papercut-21.fls".

This file is located under your PaperCut installation directory on the server, in the subdirectory `[app-path]/providers/hardware/lexmark`.

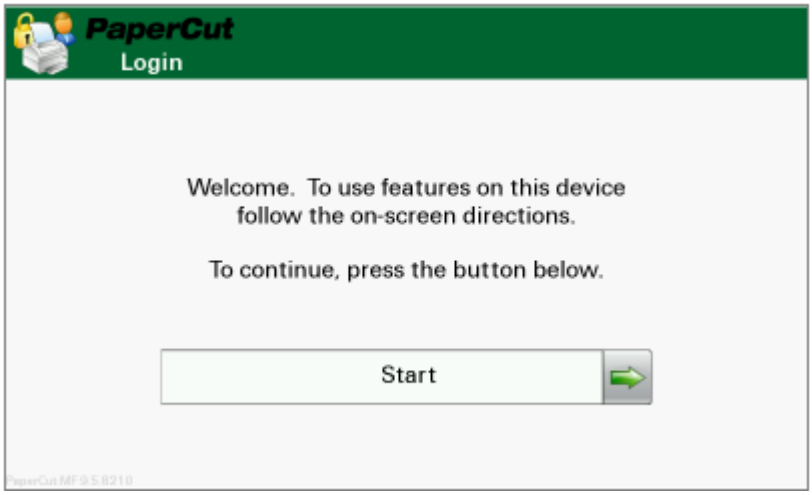
2.2.3 Installing the Embedded Application

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

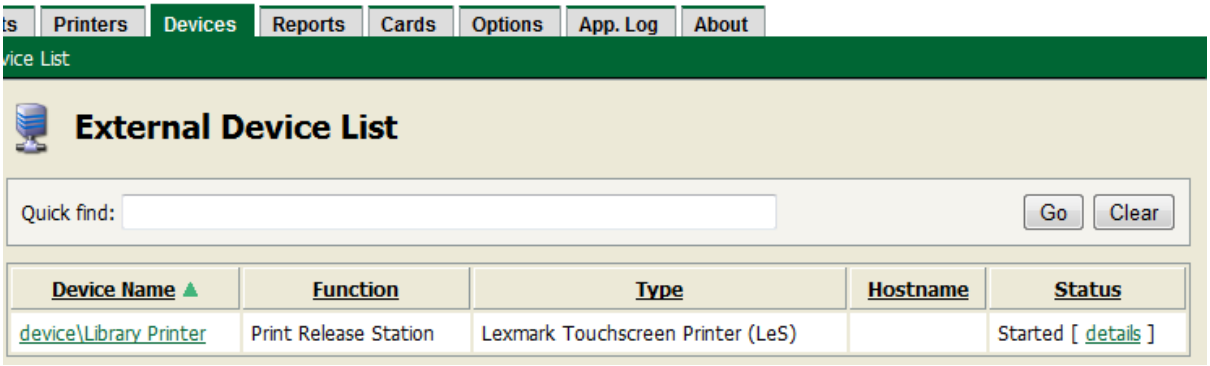
To install the application, perform the following steps:

1. On a computer, open your web browser
2. Enter the URL of the Lexmark device. E.g. http://*<lexmark-device-ip>*/
3. Select the "Settings" menu option from the left (also called "Configuration" on older devices).
4. Select "Embedded Solutions".
5. Click the "Install" button.
6. Click the "Browse …" button and select the application FLS file.
7. Click "Start Install".
8. A confirmation message will appear. Click "Return" to return to the Embedded Solutions list.
9. The list should now show an item labeled "PaperCut" and the "State" column should show "Running".
10. Click the "PaperCut" item and click on the "Configure" button that appears.
11. Enter a unique device name such as "Lexmark 1" or "Library Printer" that will later appear in PaperCut's list of devices.
12. Enter the PaperCut server's hostname or IP address under "Server Hostname".
13. Leave all other settings at their defaults and click "Apply".

14. The device will now show the PaperCut login screen.

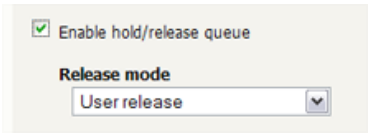


15. The Lexmark device will appear in the PaperCut administration interface under the "Devices" tab with the name you provided in the steps above.



Before continuing with the device configuration, the Lexmark printer has to be configured to hold prints in a hold/release queue:

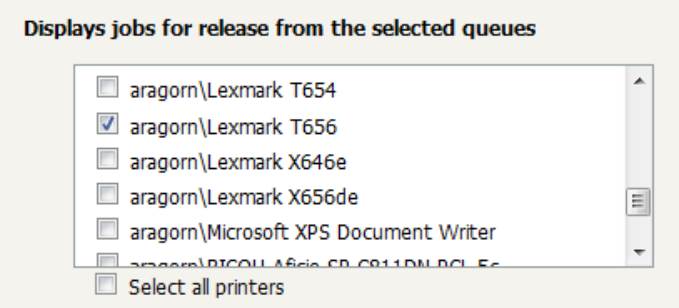
16. In PaperCut, select the "Printers" tab.
17. Select the print queue (i.e. not the 'device') for the Lexmark printer that will be used for testing.
18. Enable the "Hold/release queue" option.



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

The device can now be configured to release prints from this print queue:

20. Select the "Devices" tab.
21. Select the Lexmark device.
22. Select the print queue that was enabled for hold/release above. The Lexmark device will allow jobs on the selected queues to be released.



23. Press “OK” to save.
24. The embedded application is now successfully installed. To release prints, the users must login to the application, and select the “Print Release” button on the screen. This is discussed in detail in the next chapter.

2.2.4 Setting Logout Timeout

After logging into a device the device will show the “home screen” that presents the functions available. This screen will also show after the completion of each function. By default, Lexmark 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, respecting the following considerations:

- On one hand, the timeout should be long enough to provide the user with time to contemplate whether to continue using the device and which function to use next.
- 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 walking up to it and continue using it with the previous user’s login credentials.

To set the timeout to a different value:

- Access the Lexmark web admin interface under http://*<lexmark-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”

Lexmark devices themselves provide a functionality called “Held Jobs” that overlaps with PaperCut’s hold/release queues. “Held Jobs” should be deactivated in order to avoid confusion with PaperCut’s print release functions.

To do so:

- Access the Lexmark web admin interface under http://*<lexmark-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 a simple security configuration is recommended.

To do so:

- Access the Lexmark web admin interface under http://*<lexmark-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 some 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 “Use Profiles” to “No Security”
- This will deny users access to any functions other than print release. You may on a case by case basis revisit this setup later and re-enable other functions. In case of doubt, refuse access by setting 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 2.2). 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 quickly checking the Embedded Application's version number now matches the expected value.

3 Post-install testing

After completing installation and basic configuration it is recommended to perform some testing of the print release scenario. 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.

3.1 Test Preparation

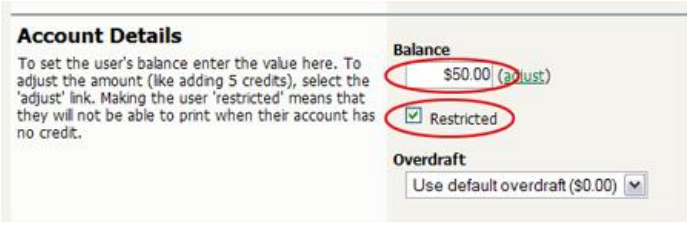
To complete the test it is recommended you use a test user called 'testuser' to perform the print release test.

To setup this user in PaperCut:

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

The next step is to configure the user. To configure 'testuser':

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



4. Press the "OK" button to save.

3.2 Print release test

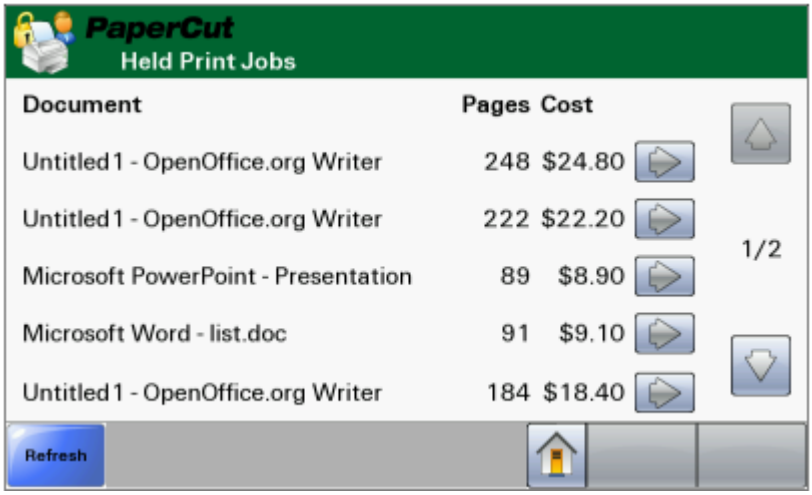
The embedded application is used for print release. For full description of PaperCut hold/release queues and release stations, please read the PaperCut manual.

1. Login to a computer workstation as 'testusersimple'.
2. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
3. 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.
4. Confirm that the username is 'testuser'.

At the device:

5. At the "Login" screen, press "Start".
6. Enter the 'testuser' username and password.
7. The device will show the home screen with a choice of functions including "Print Release".
8. Press the "Print Release" button.

9. The list of held print jobs is displayed.



10. Select the job to release by pressing the arrow next to the job.
11. Confirm the release of the print job by pressing the “Print Job” button.
12. The job will then print.
13. Try canceling a job by selecting it and then selecting the “Cancel Job” button.
14. The job will be canceled, and will not print.

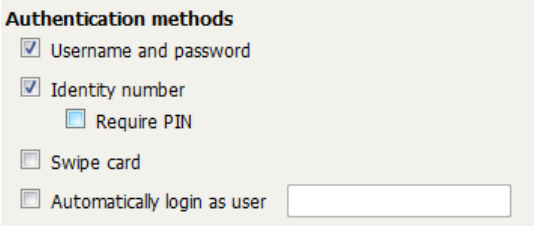
4 Configuration

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

4.1 Authentication Methods

PaperCut supports a number of different ways to authenticate users who walk-up to the devices to release prints. The default authentication method is username and password authentication (usually backed by a directory service such as Active Directory or LDAP).

The 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 A 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-	Users can swipe cards previously not used or registered at the device

association with existing user accounts	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

Description of authentication methods

4.2 Customizing Text and Messages

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

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

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 less common configuration options which are available via the 'Advanced Config' tab in the device 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 4.1 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 4.1 for details. Contact your reseller or Authorized Solution Center for help with regular expressions. You can find their contact information in your PaperCut Admin interface on the About page. 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.lexmark.header.color	See chapter 0.
ext-device.lexmark.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.lexmark.release.show-busy	Set to yes to show a warning message when users are releasing documents while the device is still busy printing. (Only on LeSF v2.1.)
ext-device.lexmark.release.show-busy.job-timeout	When above 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 above option is enabled. Specify “DEFAULT” for the default text.
ext-device.inactivity-timeout-secs	Defines how long to allow a user between key presses before they are automatically logged out. Default: 60
ext-device.card-no-regex	See chapter 0.

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\lexmark`. 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.

5.2 Custom Header Color

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

- ext-device.lexmark.header.color – the background color (type DEFAULT for the default setting of dark green)
- ext-device.lexmark.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.

5.3 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:

5.3.1 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`.

5.3.2 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. Contact your reseller or Authorized Solution Center for help with regular expressions. You can find their contact information in your PaperCut Admin interface on the About page.
    - If you would like to write your own regular expressions, here are some examples:
        - Use the first 10 characters (any character): `(.{10})`
        - Use the first 19 digits: `(\d{19})`
        - Extract the digits from between the two "=" characters in "123453=292929=1221": `\d*=(\d*)=\d*`

5.3.3 Card Number Format Converters

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

Note: Many card readers are configurable - the number format can be changed at the hardware level via utility or configuration tools. PaperCut's software-level converters are there to support card readers that don't offer this level of configuration, or where a global software-level conversion is a better choice. For example it may be quicker to do the conversion in PaperCut rather than manually reprogram 100+ readers!

Like regexes, the convertors may be defined on either a global (all devices) or on a per-device basis.

To set globally:

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

5.3.4 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.

5.3.5 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`

5.3.6 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. Contact your reseller or Authorized Solution Center to discuss development options and costs. You can find their contact information in your PaperCut Admin interface on the About page.

6 Known Limitations and Security

6.1 Known Limitations

- No limitations or issues are known at this time.

6.2 Security concerns

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

- The device's admin password (see chapter 2.2.6) always be kept secure.
- The power and network cable should be securely connected.

7 Future Development

Working on an enhanced Lexmark Embedded application that provides the following features is planned for the near future:

- Support for a wider range of card readers

8 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 being established. Check that for 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 Lexmark 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 Lexmark LCD screen?

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

What new development do you have planned?

See section 0 "

Future Development” on page 23.

A. Appendix: Supported Authentication Card Readers

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

- MagTek (USB)
- RFIdeas (USB)
- 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 Lexmark supplier for the OmniKey driver
    - PaperCut has been tested with the OmniKey driver version 2.1.2

Other card readers may be supported. Contact your reseller or Authorized Solution Center for assistance You can find their contact information in your PaperCut Admin interface on the About page.

B.Appendix: Screenshots for User Information Sheets

Many organizations aim to provide detailed step-by-step instructions to their users to guide them through device 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.