

PaperCut MF - Toshiba Embedded Manual

Contents

1	Document revision history	3
2	Installation	5
2.1	Requirements	5
2.1.1	Supported Toshiba Devices.....	6
2.2	Setup Procedure	9
2.2.1	(Mac/Linux/Novell Only) Server configuration.....	9
2.2.2	Verify Access to the Toshiba Administrative Web Interface	9
2.2.3	Networking/Firewall Configuration	9
2.2.4	PaperCut Settings.....	9
2.2.5	eBX series: Device configuration	10
2.2.6	eB3 series: Device configuration	20
2.2.7	Create Toshiba MFP device in PaperCut.....	29
2.3	Upgrading to a newer version	29
3	Post-install testing.....	29
3.1	Test Preparation	29
3.2	Scenario 1: Standard copying.....	31
3.3	Scenario 2: Copying with account selection	31
3.4	Scenario 3: Print release.....	32
4	Configuration	35
4.1	Device Function	35
4.2	Authentication Methods	35
4.3	Shared Account Selection	36
4.4	SNMP	36
4.5	Customizing Text and Messages	37
4.6	Adding application button links on the welcome page	37
5	Advanced Configuration	38
5.1	Config Editor	38
5.1	Customizing the Header Logos and Colors	40
5.1.1	Customized Logos	40
5.2	Custom Header Color	41

5.3	Configuring Swipe Card Readers	41
6	Known Limitations and Security	43
6.1	Usability and User Interface Limitations	43
6.2	Limited Authentication Options	43
6.3	Zero stop	43
6.4	Bypassing the System	44
7	Uninstalling PaperCut from the MFD	44
7.1	Uninstallation on Toshiba eBX	45
7.2	Uninstallation on Toshiba eB3	45
7.3	Further optional uninstallation steps	46
8	FAQ & Troubleshooting	47
9	Appendix A: Supported Authentication Card Readers	49
9.1	Elatec TWN3	49
9.2	Magtek Dynamag for eBX devices	50
9.3	Generic Keyboard Mode Readers	50
9.4	Configuring Swipe Card Reader Validation	51
10	Appendix B: Configuration for Apple Mac, Linux or Novell servers	55
10.1	Installing UDP redirector on Apple Mac OS X	55
10.2	Installing UDP redirector on Linux / Novell	55
11	Appendix C: Process for performing user card association	57
12	Appendix D: Device screenshots for user documentation	58
13	Appendix E: 08 Code Check list	61
13.1	eBX Codes	61
13.2	eB3 Codes	61
14	Appendix F: TopAccess Settings Check list	62
14.1	eBX TopAccess Settings	62
14.2	eB3 TopAccess Settings	62

1 Document revision history

Published date or release	Details of changes made
19.0.0	3.2.7 Create Toshiba MFP device in PaperCut; 5.4 SNMP

2 Installation

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

2.1 Requirements

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

- PaperCut is installed and running on your network. Please see the 'Installation' section of the PaperCut user manual for assistance.
- **IMPORTANT:** If your PaperCut server is installed on Linux or Apple Mac additional configuration on the PaperCut server is required. Please see the instructions in "Appendix B: Configuration for Apple Mac, Linux or Novell servers".
- Ensure that your Toshiba MFD is in the list of supported devices. Check the device lists in 2.1.1 below.
- The Toshiba devices must be directly accessible over the network by the PaperCut server (i.e. not via a NAT network).
- Verify that the Toshiba Embedded Web Browser (EWB) is enabled on your device. This is enabled through the "External Interface Enabler" (Code: GS-1020). This is an option in some markets and you should check with your Toshiba representatives.
- Have available the network name and IP address of the system running PaperCut (e.g. the print server).
- Ensure that the Toshiba MFD is connected to the network.
- Have available the network address of the Toshiba MFD. It is recommended that the MFD is configured with a static IP.

2.1.1 Supported Toshiba Devices

The following Toshiba devices are supported. The devices fall into difference generations, eB3 and eBX. Please take note of which series your device belongs to because the setup instructions differ. Below is a table with minimum recommended firmware versions.

NOTE: If using an eBX device with a new firmware version, you might consider using the newer PaperCut Toshiba integration. Please see the document “PaperCut MF - Toshiba SDK2 Embedded Manual.pdf” available on request from PaperCut. Please note that it is currently released under an *Early Access Program*.

e-BRIDGE 3	Current Field Released Firmware Version
e-STUDIO 255	T470* 330
e-STUDIO 305	T470* 335
e-STUDIO 355	(two different CCD's are supported)
e-STUDIO 455	
e-STUDIO 555	T100* 330
e-STUDIO 655	
e-STUDIO 755	
e-STUDIO 855	
e-STUDIO 2330C	T450* 330
e-STUDIO 2820C	
e-STUDIO 3520C	
e-STUDIO 4520C	
e-STUDIO 5520C	T430* 330
e-STUDIO 6520C	
e-STUDIO 6530C	
e-BRIDGE X I (ONE)	Current Field Released Firmware Version
e-STUDIO 206L	T160* 2121
e-STUDIO 256, 256SE	
e-STUDIO 306, 306SE	
e-STUDIO 356, 356SE	
e-STUDIO 456, 456SE	
e-STUDIO 306LP	T201* 2121

e-STUDIO 556, 556SE e-STUDIO 656, 656SE e-STUDIO 756, 756SE e-STUDIO 856, 856SE	T190* 2102
e-STUDIO 2040C, 2040CSE e-STUDIO 2540C, 2540CSE e-STUDIO 3040C, 3040CSE e-STUDIO 3540C, 3540CSE e-STUDIO 4540C, 4540CSE	T140* 4121
e-STUDIO 5540C, 5540CSE e-STUDIO 6540C, 6540CSE e-STUDIO 6550C, 6550CSE	T130* 4121
e-BRIDGE X II (TWO)	Current Field Released Firmware Version
e-STUDIO 2051C (WEISS LL) e STUDIO 2050C (WEISS L) e STUDIO 2550C (WEISS L)	T569* 2161 (SSD)
e STUDIO 2050C (WEISS L) e STUDIO 2550C (WEISS L)	T569* 2154 (HDD)
e-STUDIO 2555C (WEISS H) e-STUDIO 3055C (WEISS H) e-STUDIO 3555C (WEISS H) e-STUDIO 4555C (WEISS H) e-STUDIO 5055C (WEISS H)	T212* 2154
e-STUDIO 206L e-STUDIO 257, 257SE e-STUDIO 307, 307SE e-STUDIO 357, 357SE e-STUDIO 457, 457SE	T330* 1254
e-STUDIO 307LP	T360* 1054
e-STUDIO 557, 557SE e-STUDIO 657, 657SE	T320* 1254

e-STUDIO 757, 757SE

e-STUDIO 857, 857SE

e-STUDIO 5560C, 5560CSE

T340* 1254

e-STUDIO 6560C, 6560CSE

e-STUDIO 6570C, 6570CSE

e-STUDIO 477S

T290* 2154

e-STUDIO 527S

e-STUDIO 287CS

T280* 2354

e-STUDIO 347CS

e-STUDIO 407CS

NOTE: That SSD models are not supported, neither are those devices fitted with an EFI controllers. The asterix '*' used above is for the wildcard character, for example, T140*3000 would match up with the device model of T140HD0W3000.

PaperCut makes all attempts to keep the product compatibility information in this manual current. However, we make no warranties, express or implied, with respect to manufacturer's products or the interoperation with the listed PaperCut product(s). We offer 40 day trial versions of PaperCut software to assist you with compatibility testing with your network setup.

2.2 Setup Procedure

2.2.1 (Mac/Linux/Novell Only) Server configuration

When running the PaperCut application server on an Apple Mac, Linux or Novell systems some additional configuration is required. See the section “Appendix B: Configuration for Apple Mac, Linux or Novell servers” on page 55 for detailed instructions.

2.2.2 Verify Access to the Toshiba Administrative Web Interface

The Toshiba devices have an embedded web server that provides an alternate administration interface. The web interface is used to configure the MFD to connect to PaperCut.

To verify admin access:

1. On a computer, open your web browser
2. Enter the URL of the Toshiba device. E.g. <http://toshiba-device-ip/>
3. Click the “Login” link at the top right of the page.
4. Enter the device administrator username and password, and press "Login". By default this is Admin/123456.
5. Click the “Administration” tab at the top right of the page.

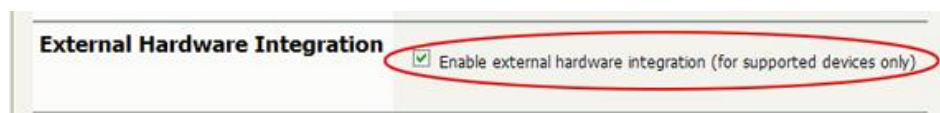
2.2.3 Networking/Firewall Configuration

Ensure that your networking/firewall configuration allows:

- Inbound connections from the Toshiba devices to the PaperCut server on ports:
 - 10389 (TCP)
 - 9191 (TCP/HTTP).
 - 162 (UDP/SNMP traps)
- Outbound connections from PaperCut to the Toshiba Device on ports:
 - 161 (UDP/SNMP)

2.2.4 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’.

2.2.5 eBX series: Device configuration

This section describes the LDAP and role configuration for eBX series devices. See section 2.1.1, for details of the devices and device series. If your device is an eB3 series device see section 2.2.6 on page 20.

2.2.5.1 Configuring the 08 “Service Mode” MFP settings

PaperCut tracks the off-the-glass copier/fax/scanner through the real-time logging facility which sends usage log data to PaperCut using SNMP traps. This must be enabled in the 08 “service mode” **only by a qualified Toshiba technician**. To do this:

1. Enter 08 service mode.
2. To enable real-time logging, change setting 3623 to 255. To do this:
 - Enter: 3623
 - Press “Start” button
 - Enter: 255
 - Press the “OK” button on the LCD screen.
3. To enable full logging, change setting 3624 to 4294967295. To do this:
 - Enter: 3624
 - Press “Start” button
 - Enter: 4294967295
 - Press the “OK” button on the LCD screen.
4. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

The user experience can be improved by making the EWB screen be the initial default screen on log in by setting the following 08 code:

1. Enter 08 service mode.
2. Enter: 9132
3. Press the “Start” button.
4. Enter: 99
5. Press the “OK” button on the LCD screen.
6. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

If using a supported USB card reader for authentication, an additional 08 setting is required. See Appendix A: Supported Authentication Card Readers on page 49 for the supported card readers and required 08 codes. To enable the card reader:

1. Enter 08 service mode.
2. Lookup the required config code in Appendix A: Supported Authentication Card Readers. e.g. for the Elatec USB reader use code 90001.
3. Change setting 3500 to the code for the given card reader. To do this:
 - Enter: 3500
 - Press “Start” button.
 - Enter the appropriate code.

- Press the “OK” button on the LCD screen.
4. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

If using card authentication, verify that the correct LDAP field is being used to lookup the card number, as follows:

1. Enter 08 service mode.
2. Check the value of setting 9398, as follows:
 - Enter 9398
 - Confirm that the value is set to either “eBMUserCard” or “pager”. If not, change it to one of these values using the onscreen keyboard and press OK.
3. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

2.2.5.2 (Optional) Change the EXTENSION button label

The button on the LCD, used to activate the embedded web browser (EWB), is labeled “EXTENSION”. If you would prefer a more descriptive label, this can be changed to any text of up to 10 characters by changing an 08 setting as follows:

1. Enter 08 service mode.
2. Change setting 9955. To do this:
 - Enter: 9955
 - Press “Start” button.
 - Enter the button description on the onscreen keyboard and press OK.
1. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

2.2.5.3 (Optional) Change the Menu/Extension button to open EWB (eBX only)

If you’d like the Menu hard-key to open the EWB directly (instead of going to the Extension page) change the 08-9985 to 1 as below. This can create a simpler user experience.

1. Enter 08 service mode
2. Change Setting 9985. To do this:
 - Enter 9985
 - Press the “Start” button
 - Enter: 1
 - Press the “Enter” button on the LCD screen.

2.2.5.4 (Optional) Populate “To” address for Scan to Email

When users log in, their email address is used in the “From” address for Scan-to-Email. To use their email address in the “To” address the following 08 code change is required:

3. Enter 08 service mode
4. Change Setting 9980. To do this:
 - Enter 9980
 - Press the “Start” button

- Enter: 1
- Press the “Enter” button on the LCD screen.

2.2.5.5 Enable SNMP real-time logs

PaperCut tracks copier usage through the Toshiba SNMP real-time logs. The device sends SNMP traps to PaperCut to notify it of copier usage. These SNMP traps are sent via UDP on port 162.

The SNMP real time logging must be enabled using the 08 service mode. For more information, see [2.2.5.1 Configuring the 08 “Service Mode” MFP settings](#).

Once the 08 service mode is changed, set the SNMP trap address as follows:

1. In TopAccess, select “Administration” -> “Setup” -> “Network”.
2. Select “SNMP Network Service”
3. Press the “SNMP Network Service” button to edit the SNMP settings.
4. Enter the IP address of the PaperCut server in “IP Trap Address 10”. **IMPORTANT:** You must use trap address 10 for the real-time log server.

SNMP V3 Trap Privacy Protocol	None
SNMP V3 Trap Privacy Password	
Enable Authentication Trap	Enable
Enable Alerts Trap	Enable
IP Trap Address1	0 0 0 0
IP Trap Address2	0 0 0 0
IP Trap Address3	0 0 0 0
IP Trap Address4	0 0 0 0
IP Trap Address5	0 0 0 0
IP Trap Address6	0 0 0 0
IP Trap Address7	0 0 0 0
IP Trap Address8	0 0 0 0
IP Trap Address9	0 0 0 0
IP Trap Address10	192 168 1 26
IP Trap Community	public
IPX Trap Address	

5. Press “OK” to save the settings.
6. **IMPORTANT:** Also press “Save” in the current Setup window to save the settings.

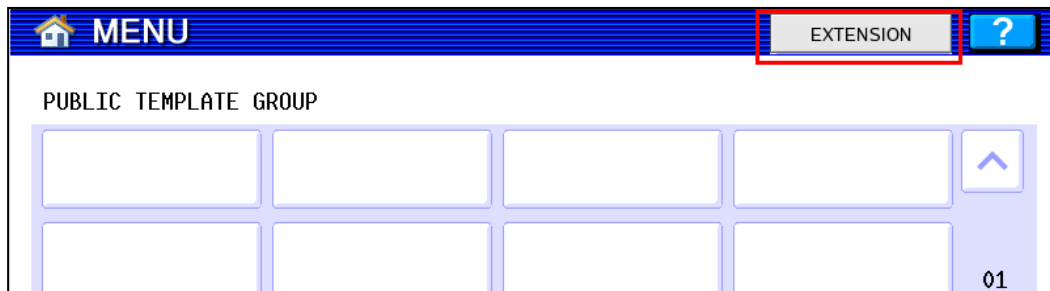
2.2.5.6 Enable the MFP Embedded Web Browser (EWB)

The Toshiba Embedded Web Browser (EWB) is an optional module licensed from Toshiba. This provides a web-based interface for print release, to select accounts/cost-centers, and to associate unknown card numbers from users. If your Toshiba MFP does not have the EWB module enabled please contact your Toshiba dealer.

To check if the EWB is enabled:

1. At the MFP device select the “Menu” hard button.

2. If the “EXTENSION” button is displayed and functional in the top right (see below), then the EWB is enabled.



To configure the EWB:

1. Login the MFP web interface (TopAccess) with your web browser.
2. Login as the “Admin” user and select the “Administration” tab.
3. Navigate to the “Administration” -> “Setup” -> “EWB” page.
4. Under the “Home Page Setting” set the “Home Page” setting as below (changing “server-address” for the address of your PaperCut server)

`http://server-address:9191/device/toshiba/`

alternatively to use an encrypted HTTPS connection (advisable when using card-association) enter:

`https://server-address:9192/device/toshiba/`

NOTE: To use HTTPS you must install an officially signed SSL certificate (e.g. from Verisign, Thawte, etc) in the PaperCut server and use the server’s DNS name. Without this the Toshiba embedded web browser will display a certificate warning message before displaying the page. See the PaperCut manual chapter “SSL/HTTPS Key Generation” for details.

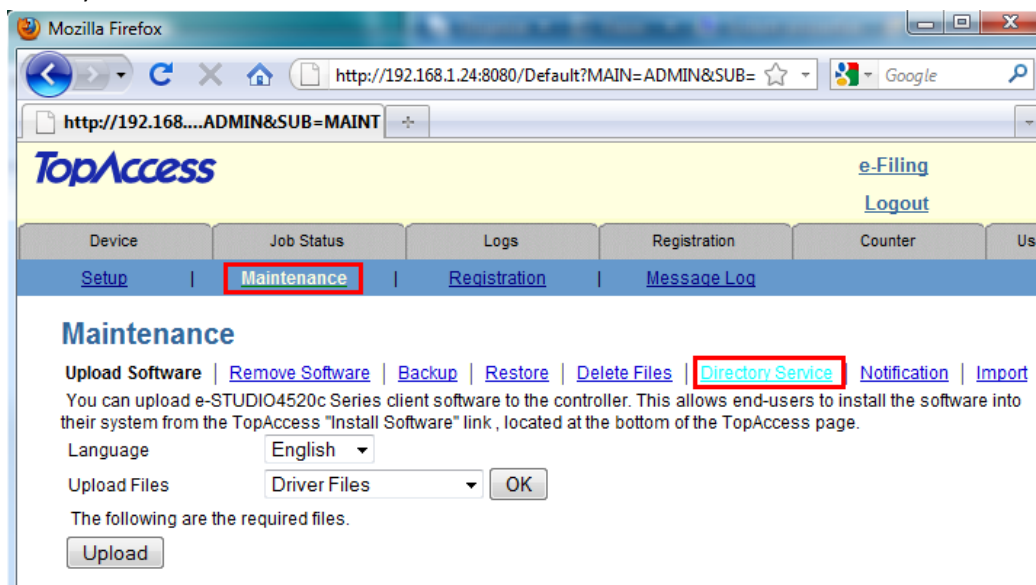
5. Press the “Save” button.

2.2.5.7 Configure MFP LDAP server

The Toshiba connects to the PaperCut using LDAP to authenticate users and validate card authentication. The MFP must be configured to establish an LDAP connection to the PaperCut server. To do this:

1. Log in to the device’s web administration (TopAccess) with a web browser.
2. Select the “Administration” tab and login as an admin user.

3. Select the “Maintenance” sub-section, and the “Directory Service” option (see below).



4. Select the new button and enter the LDAP server settings as displayed below.

Directory Service Name	Any name to identify the PaperCut LDAP server.
Server IP address	The network address of the PaperCut server.
Port	10389
Authentication	Simple Bind
Search Base	dc=pc , dc=local

User Name	uid=pc-admin,dc=pc,dc=local
Password	pc!ldap5
Enable SSL	Accept all certificates without CA
SSL Port Number	10636

IMPORTANT: You must use above Port, Authentication, Search Base, User Name, Password, Enable SSL and SSL Port Number exactly as shown above.

NOTE: If one wants to debug the LDAP protocol sequence, then one can set **Enable SSL** to *Disable* and set the **SSL Port Number** to 10389. The LDAP text data including the password will then be sent in plain text.

NOTE2: In prior releases, we required the Search Base to use “dc=toshiba” instead of “dc=pc” and the UserName was required to be “uid=tosh-admin,dc=toshiba,dc=local” instead of “uid=pc-admin, dc=pc,dc=local”. These LDAP parameters which referred to “toshiba” have been changed to be vendor neutral. However, the old settings are still supported and will continue to be supported by PaperCut.

5. Press “OK” to save the LDAP settings.
6. If you have multiple LDAP servers defined, select the newly created LDAP server as the default.

2.2.5.8(Optional) MFP LDAPS (encrypted LDAP) server settings

If you have configured PaperCut with an officially signed SSL certificate (e.g. from Verisign, Thawte, etc.) as described in the PaperCut manual chapter “SSL/HTTPS Key Generation”, then you can set the “Enable SSL” option to “Verify with imported CA certification(s)”.

If you want to use a different port number for the “SSL Port Number” then you can use a different value in TopAccess and modify the PaperCut configuration setting “ext-device.toshiba.ldaps-port” as follows:

1. Login to the PaperCut admin interface.
2. Go to the “Options” tab.
3. Select “Config Editor (Advanced)”, from the action links on the left.
4. Find the “ext-device.toshiba.ldaps-port” setting.
5. Enter the port number that was specified on the MFC in TopAccess or “-1” if you want to disable the LDAPS port in PaperCut.

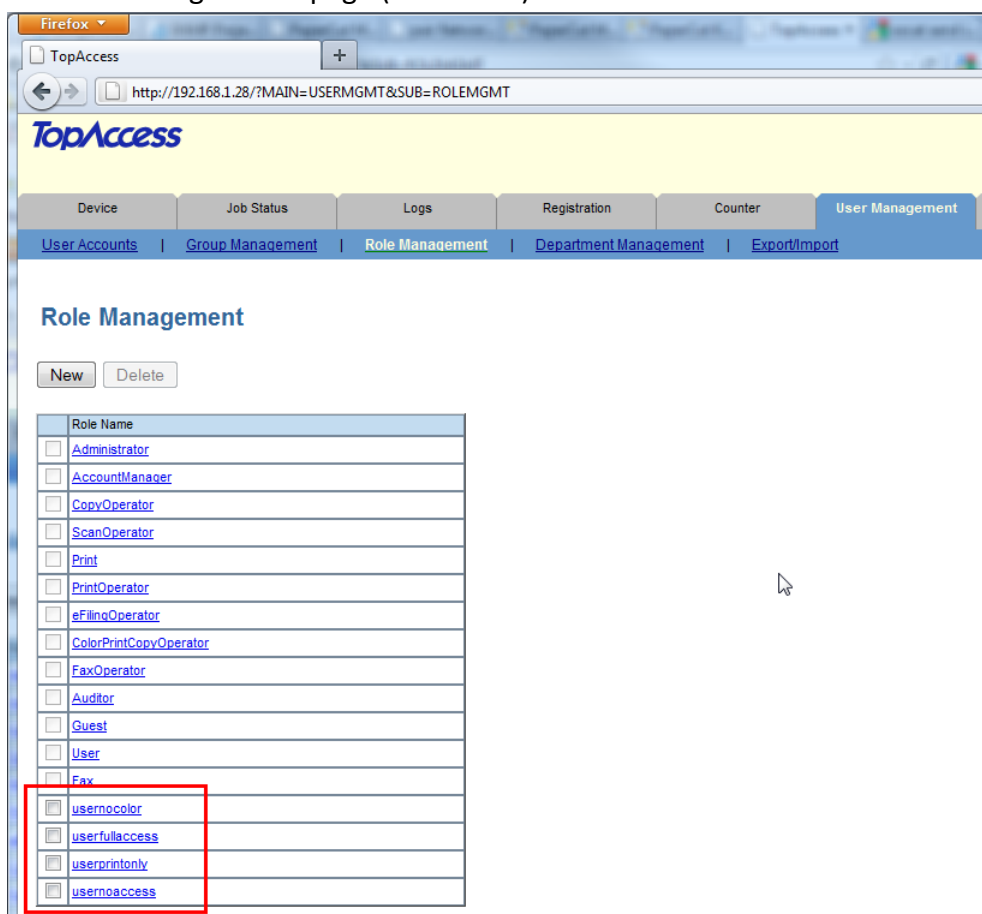
Note that if you change the LDAPS port to another number, then you must restart the PaperCut Application Server (to make it listen on the new port) and you must make sure that your server’s firewall is not blocking this port number.

2.2.5.9 Configure Role Based Access (RBAC)

The Toshiba MFP uses a role-based access system to grant access to users. For example, some users may not have access to color copying. The roles must be configured as follows:

1. Login to the device web administration (TopAccess) with a web browser.
2. Select the “User Management” tab.
3. Select the “Export/Import” subsection.

4. Press the “Import” Link.
5. In the “Combined (User information + Role + Group)” section select the following file:
[app-path]\providers\hardware\toshiba\USER_ROLE_GROUP.xml
6. Press the “Import” button.
7. In the “LDAP Role” section, select the following file:
[app-path]\providers\hardware\toshiba\LDAP_Role_Mapping.xml
8. Press the “Import” button.
9. After completing these imports the roles can be verified on the “User Management”
-> “Role Management” page (see below).



2.2.5.10 Configure Print Data Converter

If the Toshiba firmware predates version 3300, then in order to improve the Toshiba’s handling of network print jobs, a Print Data Converter file should be configured on the device. Applying the Print Data converter will guarantee that the Toshiba device will not attempt to authenticate or deny network print jobs using RBAC.

The file can be imported as follows:

1. Log in to the device web administration (TopAccess) with a web browser.
2. Select the “Administration” tab.
3. Select the “Print Data Converter” link.

4. Enable the Print Data Converter from the drop-down list.
5. In the “Import New Converter” section, select the following file:
[app-path]\providers\hardware\toshiba\Disable_Print_Authentication.xml
6. Press the “Import” button.
7. After completing this import the screen should look like the following:

TopAccess

Device | Job Status | Logs | Registration | Counter | Us

Setup | Security | Maintenance | Registration

Setup

[General](#) | [Network](#) | [Copier](#) | [Fax](#) | [Save as file](#) | [Email](#) | [InternetFax](#) | [Printer/e-Filing](#) | [Printer](#) | [Print Service](#) | [ICC](#)

Print Data Converter Setting

Print Data Converter

Import New Converter

File Name No file chosen

Current Converter

File Name	File Size	Date
Disable_Print_Authentication.xml	528	Mon Dec 12 13:11:01 2011

One caveat with doing this is that all the network print jobs will be owned by the user “printope” and by default, the real owner of the print job will not be able to delete the print job from the Job Status screen on the copier. To work around this limitation for the Job status screen, one can change an 08 code to allow anyone to delete a print job:

1. Enter 08 service mode.
2. Change setting 8726 to 1 (default is 0). To do this:
 - a. Enter: 8726
 - b. Press “Start” button
 - c. Enter: 1 (to allow all users to delete others print jobs)
 - d. Press the “OK” button on the LCD screen.

To allow the user to delete their jobs from the Private/Hold screen on the copier, the following 08 code should be set:

1. Enter 08 service mode.
2. Change setting 9236 to 3 (default is 1). To do this:
 - a. Enter: 9236
 - b. Press “Start” button
 - c. Enter: 3 (to allow users to see their own jobs and be able to delete them)

- d. Press the “OK” button on the LCD screen.


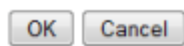
Note: since firmware version 3300, the Print Data Converter is no longer necessary. With a setting in Administration -> Security -> User Authentication Setting, it is now possible to allow a network print job to print even if the authentication fails. This setting can be seen in the screen:



2.2.5.11 Enable LDAP User Authentication

1. Log in to the device's web administration (TopAccess) with a web browser.
2. In TopAccess, select “Administration” -> “Security”.
3. Under the “User Authentication Setting” heading change the following options.
4. Change “User Authentication” to “Enable”.
5. Change “Authentication failed print job/Raw Print Job” to “Print”
6. Set the “Authentication Type” to “LDAP Authentication”
7. Choose one of the empty LDAP server entries in the table such as “LDAP Server 1”.
8. For the “LDAP Server1”, select the PaperCut LDAP server configured previously.
9. Select the “LDAP Server (Other than Windows Server)” option.

LDAP Authentication



10. Set the “Attribute type of ‘user name’” to “uid”. Then click “OK” to close the window.
11. Enable the RBAC by setting “Role Based Access using LDAP server” to “Enable”.
12. Set the RBAC LDAP server to the PaperCut LDAP server defined previously.
13. If using card authentication, set the card authentication LDAP Server to the PaperCut LDAP server previously defined.
14. Please check that the PaperCut LDAP server is specified now in 3 places:
 1. User authentication
 2. Role based access setting
 3. Card authentication setting

15. Note that if you have done a firmware update of the copier, please check that the update has not incorrectly modified any of these settings (for example, ensure that the LDAP Server's User Name attribute is still "uid").
16. Verify that the settings are all set as described (see screenshot)

User Authentication Setting

User Authentication Enable ▼

Authentication failed print job/Raw Print Job Print ▼

Auto Release on Login Disable ▼

☐ Enable Guest User

Authentication Type LDAP Authentication ▼

Primary	LDAP Server	Type	Attribute type of "User Name"
<input checked="" type="radio"/>	LDAP Server1	PaperCut LDAP Server	LDAP Server (Other than Windows Server) uid
<input type="radio"/>	LDAP Server2	Disable	
<input type="radio"/>	LDAP Server3	Disable	
<input type="radio"/>	LDAP Server4	Disable	
<input type="radio"/>	LDAP Server5	Disable	
<input type="radio"/>	LDAP Server6	Disable	
<input type="radio"/>	LDAP Server7	Disable	
<input type="radio"/>	LDAP Server8	Disable	

Role Based Access Setting

Role Based Access using LDAP server Enable ▼

LDAP Server PaperCut LDAP Server ▼

Card Authentication Setting

Primary	LDAP Server	Type	Attribute type of "User Name"
<input checked="" type="radio"/>	LDAP Server1	PaperCut LDAP Server	LDAP Server (Other than Windows Server) uid
<input type="radio"/>	LDAP Server2	Disable	
<input type="radio"/>	LDAP Server3	Disable	
<input type="radio"/>	LDAP Server4	Disable	
<input type="radio"/>	LDAP Server5	Disable	
<input type="radio"/>	LDAP Server6	Disable	
<input type="radio"/>	LDAP Server7	Disable	
<input type="radio"/>	LDAP Server8	Disable	

17. Press "Save" to confirm the changes.
18. Reboot the MFP for these settings to take effect.

At this point your device is configured; please jump to section 2.2.7 on page 29 for the PaperCut configuration.

2.2.6 eB3 series: Device configuration

This section describes the LDAP and role configuration for eB3 series devices. See section 2.1.1, for details of the devices and device series. If your device is an eBX series device see section 2.2.5 on page 10.

2.2.6.1 Configuring the 08 “Service Mode” MFP settings

PaperCut tracks the off-the-glass copier/fax/scanner through the real-time logging facility that sends usage log data to PaperCut using SNMP traps. This must be enabled in the 08 “service mode” **only by a qualified Toshiba technician**. To do this:

1. Enter 08 service mode.
2. To enable real-time logging, change setting 3623 to 255. To do this:
 - Enter: 3623
 - Press “Start” button
 - Enter: 255
 - Press the “Enter” button on the LCD screen.
3. To enable full logging, change setting 3624 to 4294967295. To do this:
 - Enter: 3624
 - Press “Start” button
 - Enter: 4294967295
 - Press the “Enter” button on the LCD screen.
4. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

The user experience can be improved by making the EWB screen be the initial default screen on log in by setting the following 08 code:

1. Enter 08 service mode.
2. Enter: 331
3. Press the “Start” button.
4. Enter: 8
5. Press the “Enter” button on the LCD screen.
6. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

If using a supported USB card reader for authentication, an additional 08 setting is required. See Appendix A: Supported Authentication Card Readers on page 49 for the supported card readers and required 08 codes. To enable the card reader:

1. Enter 08 service mode.
2. Lookup the required config code in Appendix A: Supported Authentication Card Readers. e.g. for the Elatec USB reader use code 90001.
3. Change setting 1772 to the code for the given card reader. To do this:
 - Enter: 1772
 - Press “Start” button.
 - Enter the appropriate code.

- Press the “Enter” button on the LCD screen.
4. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

If using card authentication, verify that the correct LDAP field is being used to lookup the card number, as follows:

1. Enter 08 service mode.
2. Check the value of setting 1927, as follows:
 - Enter 1927
 - Confirm that the value is set to either “eBMUserCard” or “pager”. If not, change it to one of these values using the onscreen keyboard and press OK.
3. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

2.2.6.2(Optional) Change the EXTENSION button label

The button on the LCD, used to activate the embedded web browser (EWB), is labeled “EXTENSION”. If you would prefer a more descriptive label, this can be changed to any text of up to 10 characters by changing an 08 setting as follows:

1. Enter 08 service mode.
2. Change setting 9955. To do this:
 - a. Enter: 9955
 - b. Press “Start” button.
 - c. Enter the button description on the onscreen keyboard and press OK.
3. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

2.2.6.3(Optional) Populate “To” address for Scan to Email

When users login their email address is used in the “From” address for Scan-to-Email. To use their email address in the “To” address the following 08 code change is required:

1. Enter 08 service mode
2. Change Setting 9980. To do this:
 - Enter 9980
 - Press the “Start” button
 - Enter: 1
 - Press the “Enter” button on the LCD screen.

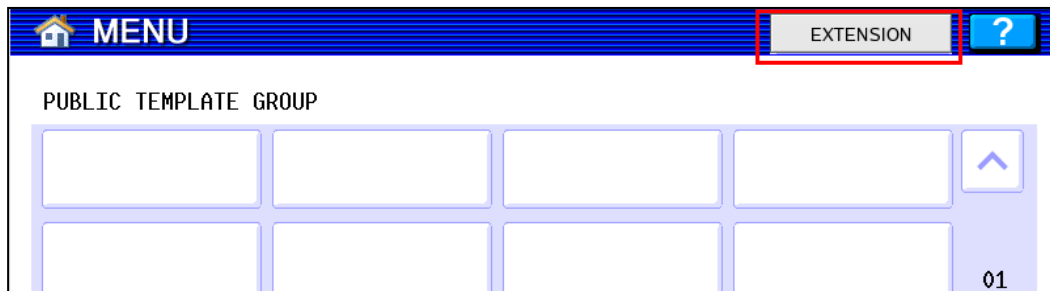
2.2.6.4Enable the MFP Embedded Web Browser (EWB)

The Toshiba Embedded Web Browser (EWB) is an optional module licensed from Toshiba. This provides a web-based interface for print release, to select accounts/cost-centers, and to associate unknown card numbers from users. If your Toshiba MFP does not have the EWB module enabled please contact your Toshiba dealer.

To check if the EWB is enabled:

1. At the MFP device select the “Menu” hard button.

- If the “EXTENSION” button is displayed and functional in the top right (see below), then the EWB is enabled.



To configure the EWB:

- Login the MFP web interface (TopAccess) with your web browser.
- Navigate to “Administration” -> “General”.
- Towards the bottom of this screen change the “EWB Setting” to “External URL”
- Enter the URL as the following (changing “server-address” for the address of your PaperCut server)

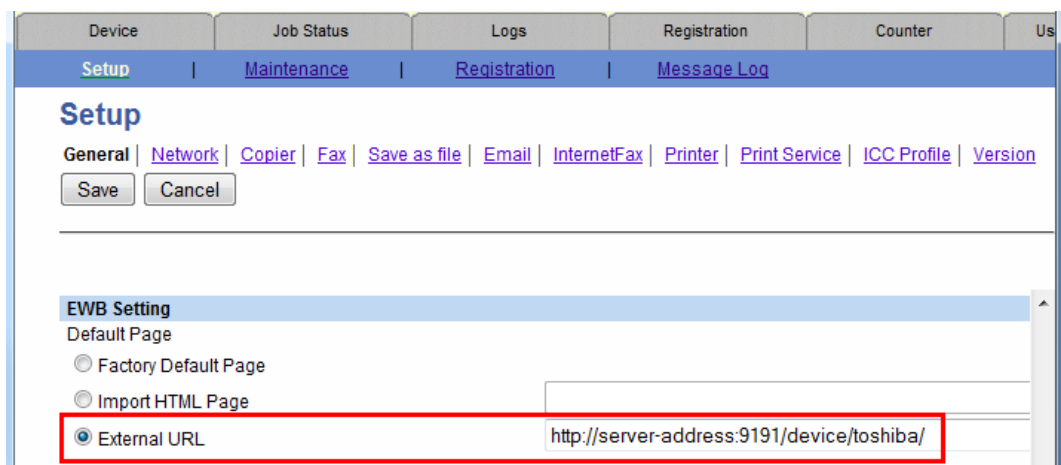
`http://server-address:9191/device/toshiba/`

alternatively to use an encrypted HTTPS connection (advisable when using card-association) use:

`https://server-address:9192/device/toshiba/`

NOTE: To use HTTPS you must install an officially signed SSL certificate (e.g. from Verisign, Thawte, etc) in the PaperCut server and use the server’s DNS name.

Without this the Toshiba embedded web browser will display a certificate warning message before displaying the page. See the PaperCut manual chapter “SSL/HTTPS Key Generation” for details.



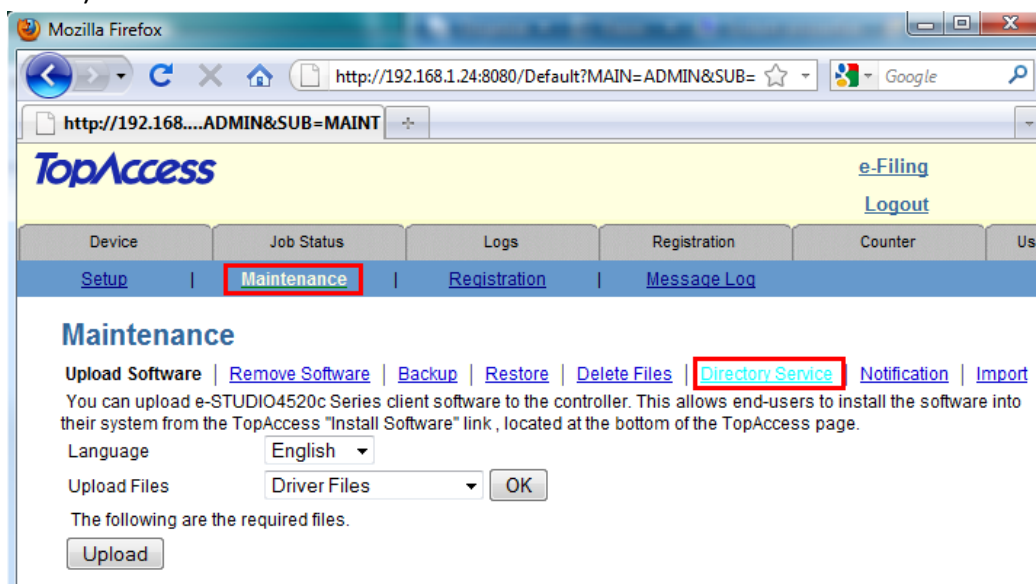
- Press “Save” button.

2.2.6.5 Configure MFP LDAP server

The Toshiba connects to the PaperCut using LDAP to authenticate users and validate card authentication. The MFP must be configured to establish an LDAP connection to the PaperCut server. To do this:

- Log in to the device’s web administration (TopAccess) with a web browser.

2. Select the “Administration” tab and login as an admin user.
3. Select the “Maintenance” sub-section, and the “Directory Service” option (see below).



4. Select the new button and enter the LDAP server settings as displayed below.

Directory Service Name

Any name to identify the PaperCut LDAP server.

Server IP address

The network address of the PaperCut server.

Port

10389

Authentication	Simple Bind
Search Base	dc=pc, dc=local
User Name	uid=pc-admin, dc=pc, dc=local
Password	pc!ldap5
Enable SSL	Accept all certificates without CA
SSL Port Number	10636

IMPORTANT: You must use above Port, Authentication, Search Base, User Name, Password, Enable SSL and SSL Port Number exactly as shown above.

NOTE: If one wants to debug the LDAP protocol sequence, then one can set **Enable SSL** to *Disable* and set the **SSL Port Number** to *10389*. The LDAP text data including the password will then be sent in plain text.

NOTE2: In prior releases, we required the Search Base to use “*dc=toshiba*” instead of “*dc=pc*” and the UserName was required to be “*uid=tosh-admin, dc=toshiba, dc=local*” instead of “*uid=pc-admin, dc=pc, dc=local*”. These LDAP parameters which referred to “toshiba” have been changed to be vendor neutral. However, the old settings are still supported and will continue to be supported by PaperCut.

5. Press “OK” to save the LDAP settings.
6. If you have multiple LDAP servers defined, select the newly created LDAP server as the default.

2.2.6.6(Optional) MFP LDAPS (encrypted LDAP) server settings

If you have configured PaperCut with an officially signed SSL certificate (e.g. from Verisign, Thawte, etc.) as described in the PaperCut manual chapter “SSL/HTTPS Key Generation”, then you can set the “Enable SSL” option to “Verify with imported CA certification(s)”.

If you want to use a different port number for the “SSL Port Number” then you can use a different value in TopAccess and modify the PaperCut configuration setting “ext-device.toshiba.ldaps-port” as follows:

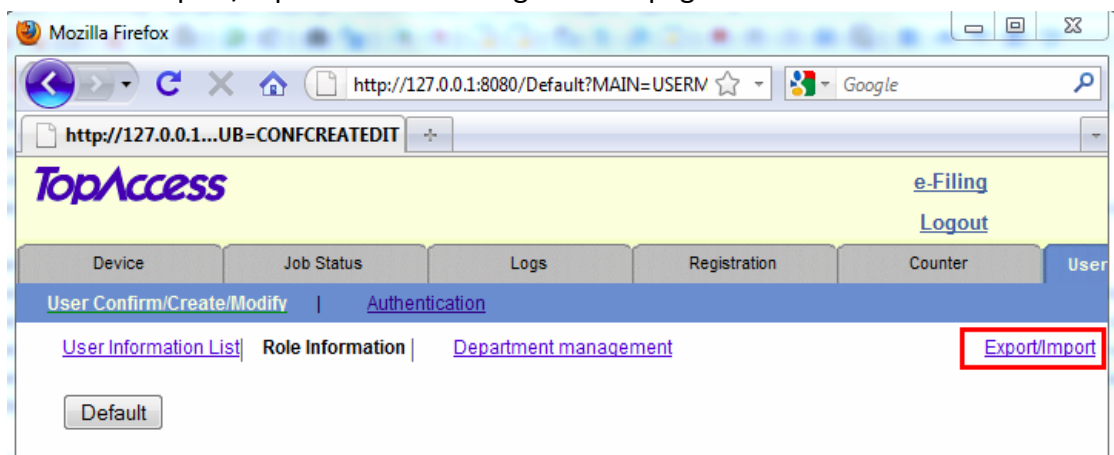
1. Login to the PaperCut admin interface.
2. Go to the “Options” tab.
3. Select “Config Editor (Advanced)”, from the action links on the left.
4. Find the “ext-device.toshiba.ldaps-port” setting.
5. Enter the port number that was specified on the MFC in TopAccess or “-1” if you want to disable the LDAPS port in PaperCut.

Note that if you change the LDAPS port to another number, then you must restart the PaperCut Application Server (to make it listen on the new port) and you must make sure that your server's firewall is not blocking this port number.

2.2.6.7 Configure Role Based Access (RBAC)

The Toshiba MFP uses a role-based access system to grant access to users. For example, some users may not have access to color copying. The roles must be configured as follows:

1. Login to the device web administration (TopAccess) with a web browser.
2. Select the "Administration" tab and login as an admin user.
3. Select "User Management" tab -> "User confirm/create/modify" -> "Role Information".
4. Press the "Import/Export" link on the right of the page.



5. Select the "Import" link.
6. Select the "Toshiba-RBAC.xml" available in the following dir on PaperCut server:
[app-path] \providers\hardware\toshiba\
7. Press the "Import" button. The list of roles should look similar to the following:

User Confirm/Create/Modify | Authentication

User Information List | Role Information | Department management | Export/Import

Default

RBAC / LDAP 'Department' attribute Setting Sample for PaperCut

Role	Settings	Copy	Email	File Share	InternetFax	Print	e-Filing	Fax	Color Output	Remote Scan
no-access	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
user-no-color	ON	ON	ON	ON	ON	ON	ON	ON	OFF	ON
user-full-access	ON	ON	ON	ON	ON	ON	ON	ON	ON	ON
user-print-only	OFF	OFF	OFF	OFF	OFF	ON	ON	ON	ON	OFF

[Go to top of this page](#)

2.2.6.8 Enable LDAP user authentication

1. In TopAccess, select "User Management" -> "Authentication".
2. Press the "User Management Setting" button
3. Select "LDAP Authentication", and change "User Authentication Enforcement" to "Print".

4. Press “Next”
5. Select the LDAP server you configured earlier.
6. Select the “LDAP server (other than windows server)” option.
7. In the “Attribute type of user name” enter: uid

8. Press the “Detail Setting” button.
9. Enable the “Role Based Access” and select the LDAP server configured earlier and press next.

10. If using USB card authentication, select the LDAP server and press “Next”.

11. Select the “Setting Address is searching from ‘User Name’ of LDAP” option

User Management Setting

Setting method of From Address field.

☐ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☒ Setting Address is searching from 'User Name' of LDAP.

[...More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

12. In the "Attribute type of 'User Name' field enter: uid

User Management Setting

Setting method of From Address field.

☐ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☒ Setting Address is searching from 'User Name' of LDAP.

[...More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

13. Change the "Mail Domain Name" to suit your organization.

14. Press the "Finish" button.

2.2.6.9 Enable SNMP real-time logs

PaperCut tracks copier usage through the Toshiba SNMP real-time logs. The device sends SNMP traps to PaperCut to notify it of copier usage. These SNMP traps are sent via UDP on port 162.

The SNMP real time logging must be enabled using the 08 service mode. For more information, see [2.2.6.1 Configuring the 08 "Service Mode" MFP settings](#).

Once the 08 service mode is changed, set the SNMP trap address as follows:

1. In TopAccess, select "Administration" -> "Network".
2. Select "SNMP Network Service"
3. Press the "SNMP Network Service" button to edit the SNMP settings.

4. Enter the IP address of the PaperCut server in “IP Trap Address 10”. **IMPORTANT:** You must use trap address 10 for the real-time log server.

SNMP V3 Trap Privacy Protocol	None			
SNMP V3 Trap Privacy Password				
Enable Authentication Trap	Enable			
Enable Alerts Trap	Enable			
IP Trap Address1	0	0	0	0
IP Trap Address2	0	0	0	0
IP Trap Address3	0	0	0	0
IP Trap Address4	0	0	0	0
IP Trap Address5	0	0	0	0
IP Trap Address6	0	0	0	0
IP Trap Address7	0	0	0	0
IP Trap Address8	0	0	0	0
IP Trap Address9	0	0	0	0
IP Trap Address10	192	168	1	26
IP Trap Community	public			
IPX Trap Address				

5. Press “OK” to save the settings.
6. **IMPORTANT:** Also press “Save” in the current Setup window to save the settings.

2.2.7 Create Toshiba MFP device in PaperCut

Now that the MFP is configured, the device can be configured in PaperCut:

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, and press "Apply" to save the change.
3. Select the "Devices" tab and press the "Create device" action link on the left.
4. Enter the device details, including the network address / IP address of the Toshiba device.
5. Select the device functions to control/log (e.g. copying, scan, fax, etc).
6. Press OK, to create the device.
7. On the device details page, change options as required. For example, here you can change the costs of copying, scanning and faxing. And select the print queues that this device will act as a "Print Release Station" for.
8. Press "OK" to save the changes.
9. The device appears on the device list. If the connection to the device is established the status column will not have an "error" state.

2.3 Upgrading to a newer version

The embedded application will be up to date when you upgrade your PaperCut installation, no further action is necessary.

3 Post-install testing

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

1. To ensure that the embedded application is working as expected
2. To familiarize yourself with the features and functionality of PaperCut and the embedded application.

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

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 the account selection enabled (i.e. to charge copying to accounts/departments/cost-centers/etc).

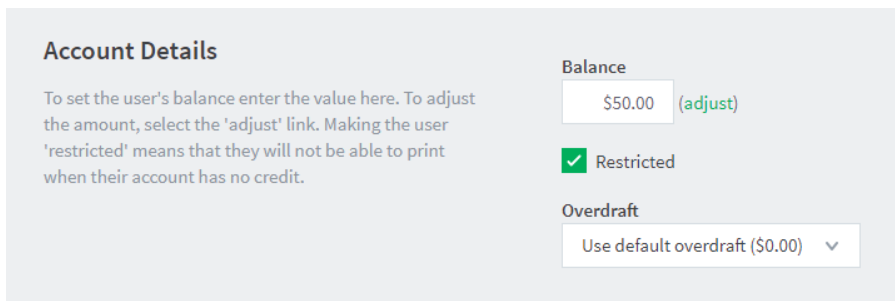
If you already have existing users for testing, then there is no need to create the users above. Instead you can use your existing users for testing.

To setup these users in PaperCut:

1. Create the 'testusersimple' and 'testuseradvanced' users 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 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".



Account Details

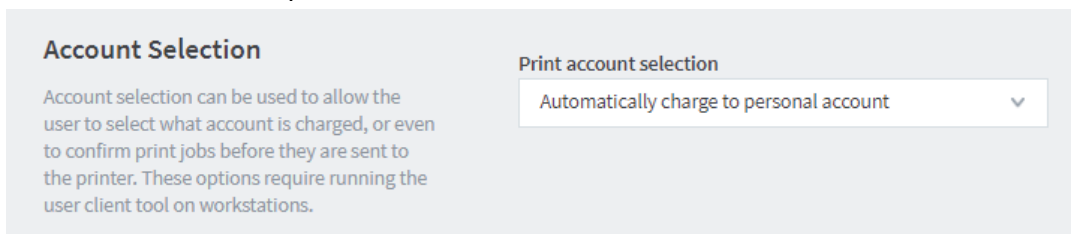
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: \$50.00 (adjust)

☒ Restricted

Overdraft: Use default overdraft (\$0.00) ▼

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



Account Selection

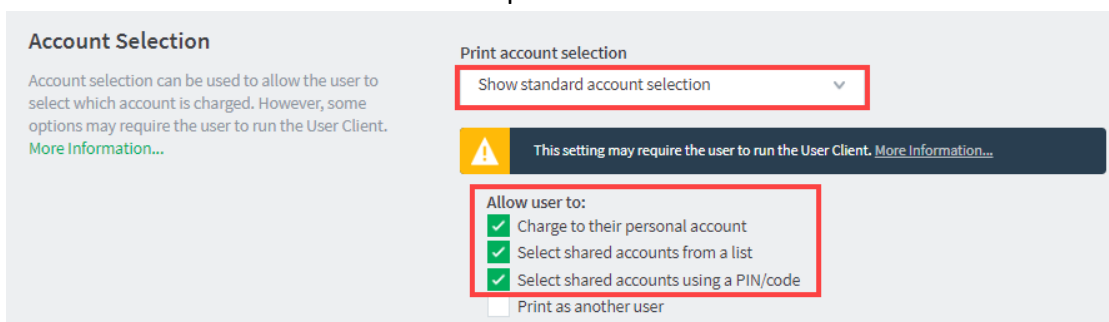
Account selection can be used to allow the user to select what account is charged, or even to confirm print jobs before they are sent to the printer. These options require running the user client tool on workstations.

Print account selection: Automatically charge to personal account ▼

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 "Show standard account selection" and select the relevant account selection options.



Account Selection

Account selection can be used to allow the user to select which account is charged. However, some options may require the user to run the User Client. [More Information...](#)

Print account selection: Show standard account selection ▼

⚠ This setting may require the user to run the User Client. [More Information...](#)

Allow user to:

- ☒ Charge to their personal account
- ☒ Select shared accounts from a list
- ☒ Select shared accounts using a PIN/code
- ☐ Print as another user

4. Press 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 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. Enter the 'testusersimple' username and password and press "Login".
2. At this point the copier will be enabled for use. Any copying/scanning/faxing performed will be charged to the logged in user.
3. Once completed, press the "Access" or "Function Clear" hard button to logout of the device.

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

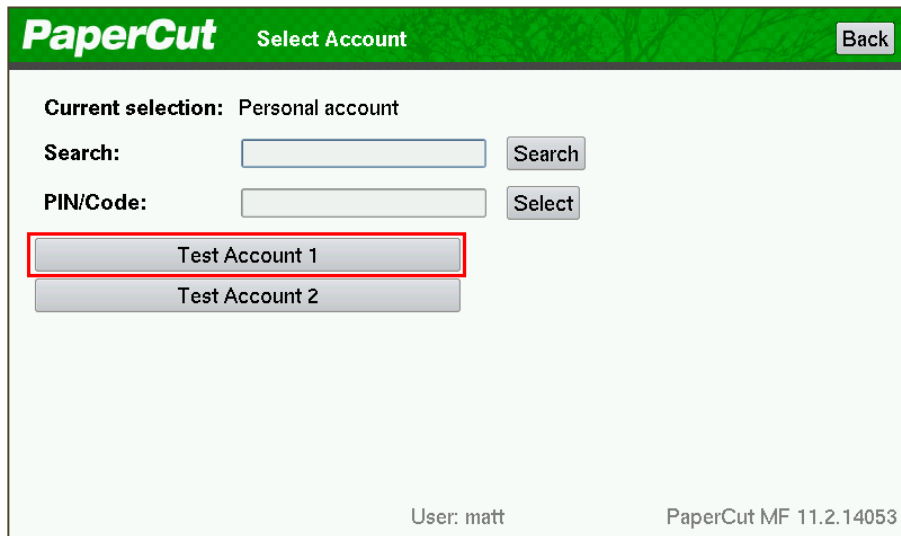
First some test accounts should be created:

1. Log 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. Press "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 the process to create another few accounts.

At the photocopier:

1. Enter the 'testuseradvanced' username and password and press "Login".

2. At this point any copies for the user will be charged to the user's personal account. To select another account open the EWB by:
 - a. Pressing the "Menu" hard key (right of the LCD)
 - b. Pressing the "EXTENSION" button.
3. The EWB will display a summary screen showing the user information. Press the "Select Account" button.
4. The screen will display the account selection options (which changes based on user settings and the number of accounts available). Select the account to allocate copying to. E.g. "Test Account 1".



5. Press the "Copy" hard key and perform some test copying.
6. Once completed, press the "Access" or "Function Clear" hard button to logout of the device.

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

3.4 Scenario 3: Print release

The embedded application may also be used for print release. For full description of PaperCut hold/release queues and release stations, please read the PaperCut manual. Skip this scenario if hold/release queues will not be used at your site.

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

1. In PaperCut, select the “Printers” tab.
2. Select the print queue (i.e. not the ‘device’) for the Toshiba MFD that is 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 Toshiba MFD’s device.
3. In the “External Device Settings”, change the “Device Function” and enable “Release Station” option.
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. You will now notice in the External Device List that the device is listed as having the function of a “Print Release Station”.
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:

1. Enter the ‘testusersimple’ username and password and press “Login”.
2. Select the “Release Held Print Jobs” option.
3. The list of held print jobs is displayed.

PaperCut Held Print Jobs					
				Refresh	Print All
				Back	
Time	Document	Pages	Cost		
11:47:22	Budget – OpenOffice.org Calc	98	\$9.80	Print	Cancel
11:47:21	Microsoft PowerPoint – Presentation	99	\$9.90	Print	Cancel
11:47:20	Microsoft Word – Document1	38	\$3.80	Print	Cancel
11:47:19	research paper.pdf	62	\$6.20	Print	Cancel
11:46:05	Budget – OpenOffice.org Calc	38	\$3.80	Print	Cancel
11:46:04	research paper.pdf	23	\$4.60	Print	Cancel
11:46:03	Microsoft PowerPoint – Presentation	93	\$9.30	Print	Cancel
11:46:02	Stats – OpenOffice.org Writer	25	\$5.00	Print	Cancel
1 / 2				Next >>	

4. Select the job to release by pressing the “Print” button next to the job.
5. The job will then print.
6. Try cancelling a job by pressing the “Cancel” button next to the job.

7. The job will be cancelled, 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 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.

Device function (e.g. copy, print release, etc)

☒ Track & control copying

Page cost
 (simple)

☐ Track & control scanning

☐ Track & control faxing

☐ Enable print release

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 and on-device printing.
Track & control scanning	The device will track scanning such as scan-to-email or scan-to-file.
Track & control faxing	The device will track the sending of faxes.
Enable 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.

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

Authentication methods

☒ Username and password
 ☒ Identity number
 ☒ Swipe card

☐ Require PIN (Not supported by this device type)
 ☒ Enable self-association with existing user accounts

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.
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.
Swipe Card->Enable self-association with existing users	If enabled, when a card number is swiped that is unknown to PaperCut the user will be allowed to login, but have no access to copier functions. They can then use the EWB to login and associate the card with their user account.

Description of authentication methods

4.3 Shared Account Selection

Shared account selection options at the MFD mirror the options presented in the User Client. 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 options available when the user prints. Selection from a list or using PIN/code are controlled at the user level via the **User Details** page. Account security/access is controlled at the account level via the **Security** tab on the **Account Details** page. For more information, see the [PaperCut MF Manual](#).

4.4 SNMP

You must configure the MFD and PaperCut MF to use SNMPv1/v2c or SNMPv3. While the MFD uses SNMP for real-time logging, PaperCut MF uses SNMP to:

- [block the release of jobs to the device when it is in error](#), and
- [retrieve the device's printer toner levels](#).

For more information about SNMP, see the [PaperCut MF manual](#).

To configure the MFD to use SNMP:

1. Ensure that the SNMP trap setting is correctly configured on the device.
2. Ensure that the 08 service mode settings have been changed.

For more information, see [2.2.5.1 Configuring the 08 “Service Mode” MFP settings](#) and [2.2.6.1 Configuring the 08 “Service Mode” MFP settings](#).

To configure PaperCut MF to use SNMP:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In the **External Device Settings**, to enable PaperCut MF to use:
 - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox is not selected (default).
 - SNMPv3, select the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox; and enter the following fields:
 - **Context name** – Enter **MFP**.
 - **Username, Privacy password, Authentication password** - If these values are available at the device web interface, then use the same values. If not, leave them blank or enter your own value.
 - **Authentication protocol** – Select either **MD5** or **SHA**.
 - **Privacy protocol** – Select either **DES** or **AES**.
5. Click **Apply**.

4.5 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 on the EWB screen that shows the user details.

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

4.6 Adding application button links on the welcome page

PaperCut allows one or two buttons to be added to the initial PaperCut welcome page which allows the Embedded Web Browser (EWB) to redirect to configured URLs. This can be used, for instance, to go to a 3rd party scan connector application. For more details about the configuration variables to set, please refer to the Advanced Configuration section and modify the configuration variables prefixed by “*ext-device.toshiba.app-button*”.

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.toshiba.welcome-text	The text displayed on the 'welcome screen' (the screen displayed after pressing 'Start' from the ready screen). This text can be used to provide specific information about logging in to the device. Default: DEFAULT (uses the default application text).
ext-device.toshiba.locale-override	Used to override the language displayed on the device. This is the 4-letter language code for the required language. E.g. "FR_fr" for French.
ext-device.card-no-regex	See chapter section 5.3.
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.release-columns	<p>The columns to display in the print release screen. This is a comma separated list of column names. The valid column names are:</p> <ul style="list-style-type: none">time – the time of the jobuser – the username of the user that printeddocument – the document namepages – the number of pages in the jobcost – the cost of the jobclient – the client machine namedatetime – the date & time of job <p>When set to DEFAULT the following are used: Secure print release mode: time, document, pages, cost. Release any mode: time, user, document, pages, cost</p>

ext-device.toshiba.header-font-color	The color used for the font in the header. The color should be entered as a HTML RGB value in the format #RRGGBB. NOTE: The Toshiba has a limited color palette (the 256 web safe palette).
ext-device.toshiba.header-background-color	The color used for the background color header. The color should be entered as a HTML RGB value in the format #RRGGBB. NOTE: The Toshiba has a limited color palette (the 256 web safe palette).
ext-device.toshiba.limit-reference.duplex	Used at log in time, to assume whether the copying is going to be duplex or not. This is used in order to decide if we have enough quota to do a single copy.
ext-device.toshiba.limit-reference.grayscale	Used at log in time, to assume whether the copying is going to be grayscale or not. This is used in order to decide if we have enough quota to do a single copy. By default, this is set to <i>N</i> and we assume a color copy.
ext-device.toshiba.limit-reference.paper-size	Used at log in time, to assume what page size the copying is going to use. This is used in order to decide if we have enough quota to do a single copy. By default, for the United States this size is <i>Letter</i> and elsewhere it is <i>A4</i> .
ext-device.toshiba.hide-cancel-job-button	When set to “Y” it will ensure that the Cancel buttons are never displayed on the Print Release web page. Default: N (the cancel buttons will be shown for release jobs)
ext-device.toshiba.direct-to-release-page	When set to “Y”, upon login the user will go direct to the print release page (assuming the device is configured for print release) and skip the welcome screen. Default: N (it will go to the welcome page on login)
ext-device.toshiba.app-buttons.enabled	When set to “Y” it will enable the application buttons on the welcome screen. The label(s) and URL(s) need to then be defined. Either 1 or 2 buttons can be set. Default: N (application buttons will not be shown by default)
ext-device.toshiba.app-buttons.heading	The text displayed for the heading at the bottom of the welcome screen to introduce the application buttons. Default: DEFAULT (use the default heading text)

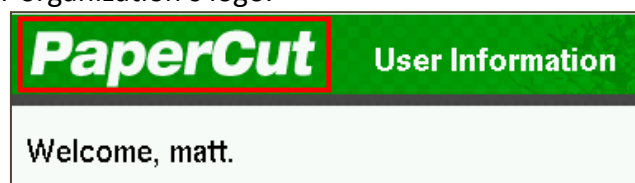
ext-device.toshiba.app-button1.label	<p>OPTIONAL: The application label for the 1st button (if needed).</p> <p>Default: NONE (the button will not be displayed if this is set to "NONE")</p>
ext-device.toshiba.app-button1.url	<p>OPTIONAL: The application URL for the 1st button (if needed).</p> <p>Default: NONE (need to change to a valid URL if you want to use this button)</p>
ext-device.toshiba.app-button2.label	<p>OPTIONAL: The application label for the 2nd button (if needed).</p> <p>Default: NONE (the button will not be displayed if this is set to "NONE")</p>
ext-device.toshiba.app-button2.url	<p>OPTIONAL: The application URL for the 2nd button (if needed).</p> <p>Default: NONE (need to change to a valid URL if you want to use this button)</p>
ext-device.toshiba.show-job-status-button	<p>Determines whether or not the Job Status button is displayed on the Print Release page.</p> <ul style="list-style-type: none">• Y—show the Job Status button on the Print Release page if the Embedded Web Browser (EWB) version is 2.1.37+, ext-device.toshiba.show-printer-error is "Y", and there is no printer error.• N—Do not show the Job Status button on the Print Release page. <p>Default: "Y"</p>

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 a single header logo (as shown below). This logo can be replaced with your organization's logo.



This shows one logo outlined in red. The images must be saved in the PNG format. The PaperCut logo has the size of 200 pixels wide by 42 pixels high. It is important that your logo has a height of 42 pixels, but the width can vary.

This custom logo must be stored on the PaperCut server in the location:

[app-path]\server\custom\web\device\toshiba\header-logo.png

Please create the folders as required if they do not already exist.

5.2 Custom Header Color

The header colors are defined in the Advanced Config settings as described in Section 5.1. See the settings for “ext-device.toshiba.header-font-color” and “ext-device.toshiba.header-background-color”.

NOTE: The Toshiba devices have a limited color palette (the 256 color web-safe palette).

5.3 Configuring Swipe Card Readers

Swipe cards contain numbers which are 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 two ways:

- 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.
- 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” in the PaperCut Admin Console. Open the Admin Console and select the Options tab, then select “Config Editor (Advanced)” from the left menu. 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*`

6 Known Limitations and Security

6.1 Usability and User Interface Limitations

The Toshiba SDK provides no ability to customize the device login process and workflow. Instead PaperCut leverages the device's built-in authentication by implementing a custom LDAP server. The Toshiba device connects to the PaperCut LDAP server to perform username/password and swipe card authentication.

After the user is authenticated they are either taken straight to the "copier" screen or the Embedded Web Browser (EWB) screen (if you enabled the 08 code). However, at any stage the user is free to go to the copier screen by hitting the "copier" button and PaperCut has no way of preventing this other than removing copier permissions. If the user wants to go back to the PaperCut screen in the Embedded Web Browser, they must press the "Menu" hard key and then the "EXTENSION" button. This is not an ideal user experience, and may require some user training to overcome.

An example of when this is a problem is if the user should not have permission to charge copying to their personal user account, but instead should select an account. As PaperCut cannot force this account selection, it defaults to charging to the personal account. As a possible work-around you may configure a "Default Shared Account" to preselect a particular shared account at login.

Toshiba are aware of this issue and aim to improve their SDK for future devices.

6.2 Limited Authentication Options

Similar to section 6.1 above, the Toshiba SDK does not allow for customizing the authentication process. For this reason, PaperCut has the following limitation with login/authentication:

- No option for Identity number and PIN authentication (only username/password is available).
- No option for PIN entry when performing card authentication.

6.3 Zero stop

In an ideal implementation, PaperCut would be able to control exactly how many pages a user can copy and always prevent the user from overdrawing his/her account. The Toshiba embedded environment has some limitations in the controlling of copying/scanning/faxing. PaperCut will only enable the copier when an authorized user has authenticated at the device (and has enough credit to begin copying). If a restricted user attempts to login and they have no available credit, they will be denied access to photocopying. However, the Toshiba environment has the following limitations:

- Once the user starts copying, it is not possible to forcibly stop the copying and log them out of the system.

The implication of this limitation is:

- Restricted users with available credit can start copying and continue copying even once they have used their credit. Their copier usage will still be recorded in PaperCut

and the cost will be deducted from their account (which will go into negative balance).

This is a limitation of the Toshiba embedded platform.

6.4 Bypassing the System

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

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

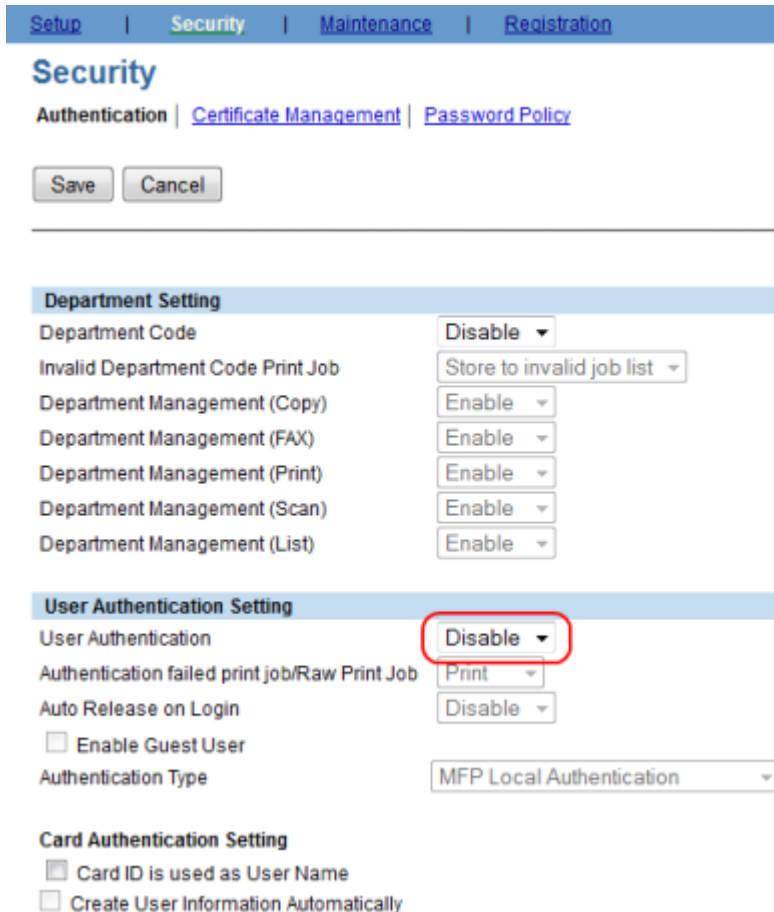
7 Uninstalling PaperCut from the MFD

In order to stop the Toshiba MFD from trying to authenticate with PaperCut and allow free copying on the device, the simplest option is to disable the "User Authentication Setting." If all you do is this step, then it is very simple to re-enable the MFP for PaperCut again if you change your mind.

7.1 Uninstallation on Toshiba eBX

To disable the PaperCut authentication follow these steps:

1. Log in to the device's web administration (TopAccess) with a web browser.
2. In TopAccess, select "Administration" -> "Security".
3. Under the "User Authentication Setting" heading change "User Authentication" to "Disable".



The screenshot shows the 'Security' configuration page in the PaperCut MF web administration interface. The page has a blue header with navigation tabs: 'Setup', 'Security' (selected), 'Maintenance', and 'Registration'. Below the header, the 'Security' section is active, with sub-tabs for 'Authentication', 'Certificate Management', and 'Password Policy'. There are 'Save' and 'Cancel' buttons at the top. The main content area is divided into three sections: 'Department Setting', 'User Authentication Setting', and 'Card Authentication Setting'. In the 'User Authentication Setting' section, the 'User Authentication' dropdown menu is highlighted with a red circle and set to 'Disable'. Other settings in this section include 'Authentication failed print job/Raw Print Job' (set to 'Print'), 'Auto Release on Login' (set to 'Disable'), 'Enable Guest User' (unchecked), and 'Authentication Type' (set to 'MFP Local Authentication'). The 'Department Setting' section includes 'Department Code' (set to 'Disable'), 'Invalid Department Code Print Job' (set to 'Store to invalid job list'), and several 'Department Management' options (Copy, FAX, Print, Scan, List) all set to 'Enable'. The 'Card Authentication Setting' section includes 'Card ID is used as User Name' and 'Create User Information Automatically', both of which are unchecked.

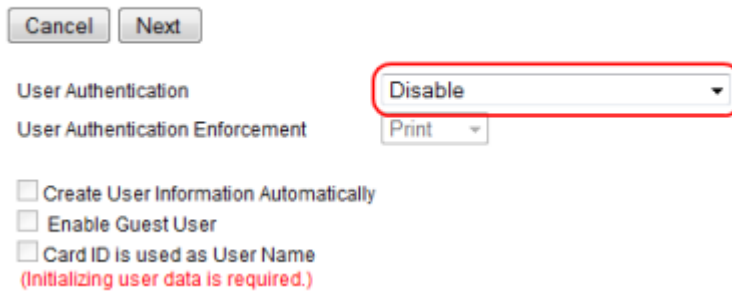
7.2 Uninstallation on Toshiba eB3

To disable the PaperCut authentication follow these steps:

1. Log in to the device's web administration (TopAccess) with a web browser.
2. In TopAccess, select "User Management" -> "Authentication".
3. Press the "User Management Setting" button

4. Select “LDAP Authentication”, and change “User Authentication” to “Disable”.

User Management Setting



Cancel Next

User Authentication **Disable**

User Authentication Enforcement Print

☐ Create User Information Automatically

☐ Enable Guest User

☐ Card ID is used as User Name

(Initializing user data is required.)

7.3 Further optional uninstallation steps

Theoretically, you could reverse all the steps that you followed during the installation process. You could revert the 08 codes back to what they were and change all the Top Access menu options back to what they were. However, disabling the authentication would be the prime thing that is required. Some other steps to be more complete could include:

- Removing the EWB URL so that the menu option doesn't try to contact the PaperCut application server
- Disabling the real time logs and their SNMP traps

8 FAQ & Troubleshooting

My Toshiba device is not logging any copy/fax/scan jobs? What's wrong?

There are a number of possible problems. Check the following:

- In the PaperCut admin site, go to the "Devices" tab and select the device:
 - Verify that the "Device hostname / IP" is correct.
 - Verify that the appropriate "Device Functions" are enabled. i.e. To track faxes ensure "Track & control faxing" is enabled.
 - Check the Device Status on this page (or in Status column of Device List) to ensure no errors are occurring.
- Windows Only: Ensure that no other services are listening for SNMP traps on port 162. Only one application can listen for SNMP traps, and if another application is already listening for traps then PaperCut will not be able to receive these notifications from the MFD. If PaperCut cannot listen to trap port 162, a message will be logged in the "Application Log" tab – "Unable to initialize SNMP trap listener on port: 162.". If this is occurring find and stop the service using UDP port 162 and then restart PaperCut. One common service that listens to SNMP traps is the Microsoft "SNMP Trap" service – stop and disabled this service. To find what application is using the port you can run the following command at the command prompt:

```
netstat -anb -p UDP
```

- Verify that the SNMP trap setting is correctly configured on the device.
- Verify that the 08 service mode settings have been changed..
- Verify that PaperCut can query SNMP values from the device:
 - Ensure SNMP is enabled and the "public" community allows read-only access.
 - Ensure your network/firewalls allow SNMP traffic between PaperCut and the device (both directions).

The card reader isn't working? What's wrong?

Firstly ensure that you are using a compatible card reader (see Appendix A on page 49).

If you are using a compatible card reader the most likely cause is a configuration issue:

- Make sure the card reader is connected while the device is booting up. Try rebooting the device.
- Check the 08 codes used to enable the card reader (e.g. 1772 on eB3 and 3500 on eBX)
- Check that correct LDAP server is selected in the "card reader" setting in the LDAP authentication settings in TopAccess.

What is the IP address of my PaperCut Server?

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

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.

The Role Based Access Controls (RBAC) do not appear to be working

Try uploading the XML files again as per the instructions for your eB3 or eBx device. Also confirm you are running a compatible firmware. Version 310 on eB3 devices is known to not correctly use RBAC settings.

Login on my Toshiba device is very slow

This can be caused by incorrect network settings on the copier such as incorrect DNS servers, subnet masks and similar. We recommend checking all network settings. If this does not resolve the issue you can force network settings to be reset to default on eB3 by initializing the '08 Service Modes' 947 and then 693.

Your authorized Toshiba technician can advise on how to initialize these settings.

PaperCut MF is not tracking my print jobs on Windows 2008 R2 Server

Windows 2008 R2 Server firewall has the default rule SNMP Trap Service (UDP Inbound on port 162) set to No with access only by the snmptrap.exe group. This causes SNMP packets containing job data from the device to be dropped and tracking is not performed by PaperCut.

To fix this issue, create a new rule in the "Windows Firewall with Advanced Security" tool to allow SNMP packets on UDP port 162.

9 Appendix A: Supported Authentication Card Readers

The Toshiba devices support the following card reader types. Each card reader type requires a different 08 service mode setting configuration which is typically done in the section “Configuring the ‘08 Service Mode’ MFP settings” and is described in the tables below.

eBX device 08 codes:

Card Reader Type	08 service code	service mode setting
Elatec TWN3	3500	90001
Magtek Dynamag	3500 3501	70001 1 or 2 or 3 (see section 9.2)
e-Bridge IDGATE - HID iClass	3500	40002
e-Bridge IDGATE - Mifare	3500	30001
Generic Keyboard mode readers	3500	60001

eB3 device 08 codes:

Card Reader Type	08 service code	service mode setting
Elatec TWN3	1772	90001
e-Bridge IDGATE - HID iClass	1772	40002
e-Bridge IDGATE - Mifare	1772	30001

NOTE: e-Bridge IDGATE in the table refers to Toshiba’s own brand of card readers.

9.1 Elatec TWN3

The Elatec TWN3 card reader can support a large variety of card types including:

- HID PROX (HID PROX)
- HID iCLASS (HID iCLASS)
- Multi125 (EM410x, HITAG 1, HITAG 2, HITAG S, EM4150, T5567/Q5)
- Inditag (Indala)
- MIFARE (MIFARE, Ultralight, MIFARE Mini, MIFARE 1k/4k, MIFARE DESfire)
- Legic (Legic Prime, Legic Advant)

For this card reader set 08 service mode setting to: **90001**. For EB3 series use 08 code **1772**. For the eBX series use 08 code **3500**.

NOTE: The Elatec TWN3 may require special firmware to use on the Toshiba devices. This is available from PaperCut. Download and firmware upgrade instructions can be found on the PaperCut knowledge base at the link below:

<http://www.papercut.com/kb/Main/ElatecFirmwareForToshibaMFP>

9.2 Magtek Dynamag for eBX devices

Toshiba eBX devices have magnetic card reader support for the Magtek Dynamag card reader. This is set using the 08 code of **3500** with a mode setting of **70001**. As well as setting the type of reader using the **3500** code, one also needs to set the **3501** code to specify which track data to use as specified in the table below.

Track data	08 service mode setting 3501
Use track 1 data	1
Use track 2 data	2
Use track 3 data	3

When entering the track number (for example, track 2 has been used for the banking industry), you will be shown boxes with the letters A to F. Please ignore this and just enter one of the digits 1 to 3 on the key pad. Then press OK. You will be asked to repeat this for confirmation and so just enter the same digit again and press OK.

9.3 Generic Keyboard Mode Readers

Card readers in generic keyboard mode are supported with recent firmware. Below is a list of firmware required for some of the Toshiba models.

e-BRIDGE X (eBX) series	Minimum Firmware Level by Series
e-STUDIO 2050C, 2550C	T569* 1518 (with hard disk) T210* 1518 (without hard disk)
e-STUDIO 2051C	T230* 1518
e-STUDIO 287CS, 347CS, 407CS	T280* 2146

The following card reader models below have been tested and are supported in generic keyboard mode. Other models not in the table may be supported by calling a Toshiba technician to make the necessary change (to register the new card reader's Product ID (PID) and Vendor ID (VID)).

Vendor	Product Name
Elatec	TWN4 TWN3
RFIdeas	pcProx Plus pcProx Enroll iCLASS ID# pcSwipe Enroll
IDTECH	OMNI combined barcode and magnetic stripe reader
Datalogic	Magellan 800i
Magtek	
Cartadis	TCM2MIFARE/HID TCM3 13.56 MIFARE TCM3 125KK HID
FTDI	FT232R USB UART IC USB UART IC

9.4 Configuring Swipe Card Reader Validation

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).

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 in 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 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*`

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 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) then 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 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`

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.

10 Appendix B: Configuration for Apple Mac, Linux or Novell servers

The PaperCut integration with Toshiba devices makes use of SNMP traps to receive usage information from the device (e.g. copier/scan/fax usage). SNMP traps are delivered over the network to the PaperCut application server over UDP on port 162.

On Unix-based systems like Mac and Linux, only privileged processes (i.e. those running as the superuser “root”) have access to open network ports below 1024. This means that PaperCut is unable to receive these SNMP traps because the PaperCut process runs as a non-privileged user (typically a user named “papercut”).

One possible approach to solve this would be to run the PaperCut application server as the “root” superuser. We chose to not use this approach because running applications as “root” goes against security best practices and could make the system vulnerable to security breaches.

The approach taken was instead to:

1. Have PaperCut listen for SNMP UDP packets on a non-privileged port (10162)
2. Run a light-weight program as root that simply redirects packets from port 162 to the port PaperCut is listening on (10162).

The administrator must manually configure this UDP redirector to run as root at system boot time. The instructions for this are outlined in the sections below.

10.1 Installing UDP redirector on Apple Mac OS X

The UDP redirector must be run as root and started at system boot time. The simplest way to achieve this on the Mac is to add the UDP redirector to the `/etc/rc.local` file. This can be done by entering the following commands in the Terminal (use copy and paste!!):

```
sudo sh -  
echo '#!/bin/sh' >> /etc/rc.local  
echo '"/Applications/PaperCut MF/server/bin/mac/pc-udp-redirect" &' >> /etc/rc.local  
chmod 755 /etc/rc.local  
exit
```

ADVANCED NOTE:

The above simply creates an `/etc/rc.local` file, adds the command to run the redirector and sets execute permissions on the file. If you are familiar with editing system config files you can do the same with a tool like the vi text editor.

Alternate approach:

An alternative to using the UDP redirector is to make use of an iptables forwarding rule like the following:

```
iptables -t nat -A PREROUTING -p udp --dport 162 -j REDIRECT --to-port 10162
```

10.2 Installing UDP redirector on Linux / Novell

The UDP redirector must be run as root and started at system boot time. There are a variety of ways to achieve this, but the simplest and recommended way is to run the UDP redirector from the `/etc/rc.local` script.

To do this:

1. Open the file `/etc/rc.local` in a text editor. (You will typically need to be root to edit this file).

2. Add one of the following lines to the script (depending if you're running 32-bit or 64-bit Linux):

For 32-bit systems:

```
/home/papercut/server/bin/linux-i686/pc-udp-redirect &
```

For 64-bit systems:

```
/home/papercut/server/bin/linux-x64/pc-udp-redirect &
```

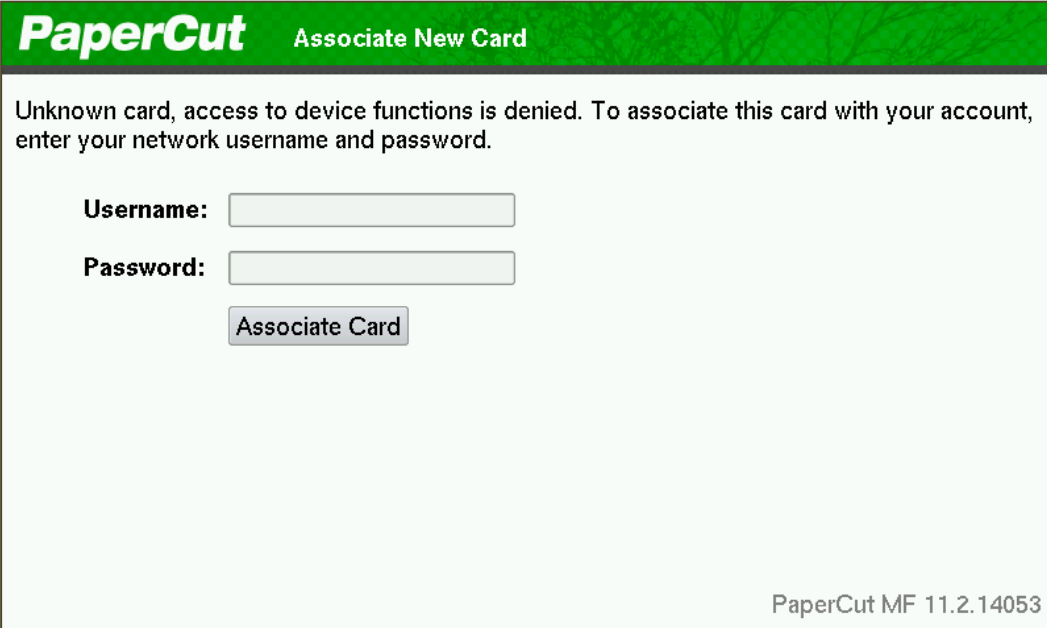
(If you have installed PaperCut into a different directory you may need to change the above paths)

3. Reboot the system and verify that the `pc-udp-redirect` program is running after the reboot.

11 Appendix C: Process for performing user card association

This section describes the process of how a user can associate a new card with their PaperCut account on the Toshiba devices.

1. Present card at the MFP reader (should hear a beep)
2. If the web screen is not set as the default, bring up the web interface (EWB) by doing:
 - a. Press MENU hard key on the MFP
 - b. Press the EXTENSION icon (or other name as assigned)
3. The following screen is displayed to allow the user to authenticate with a username and password.



PaperCut Associate New Card

Unknown card, access to device functions is denied. To associate this card with your account, enter your network username and password.

Username:

Password:

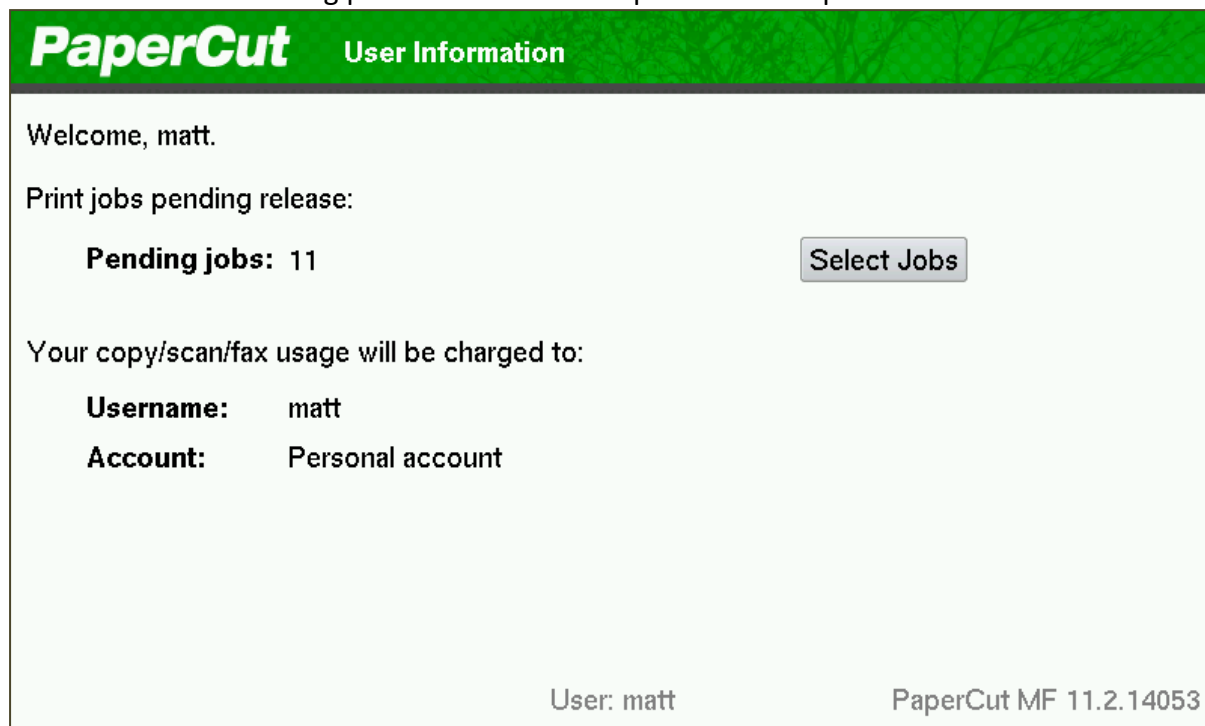
PaperCut MF 11.2.14053

4. Enter the username and password. If the association is successful the user is notified on the LCD screen.
5. Logout (press FC twice).

At this point the card has been associated with the user's account. Swiping the card again will allow them to login using the card.

12 Appendix D: Device screenshots for user documentation

This section contains some screenshots that may be used for end-user documentation.
Welcome screen showing personal account and print release options:



PaperCut User Information

Welcome, matt.

Print jobs pending release:

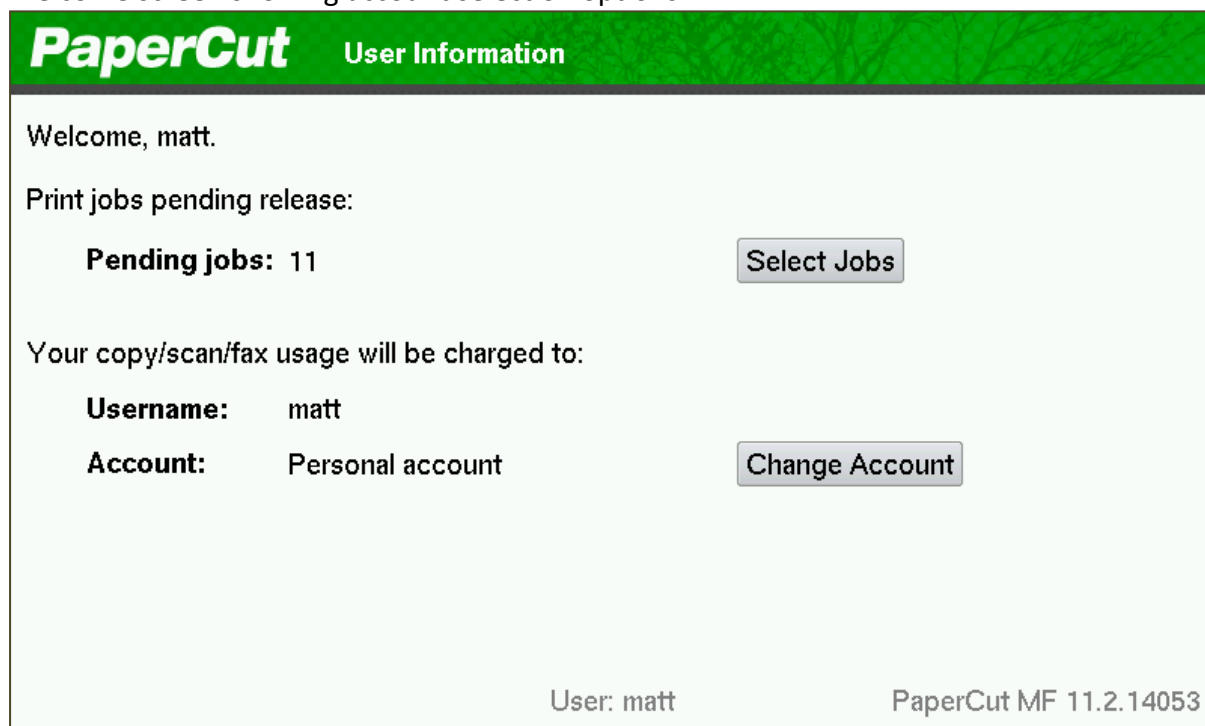
Pending jobs: 11 [Select Jobs](#)

Your copy/scan/fax usage will be charged to:

Username: matt
Account: Personal account

User: matt PaperCut MF 11.2.14053

Welcome screen showing account selection options:



PaperCut User Information

Welcome, matt.

Print jobs pending release:

Pending jobs: 11 [Select Jobs](#)

Your copy/scan/fax usage will be charged to:

Username: matt
Account: Personal account [Change Account](#)

User: matt PaperCut MF 11.2.14053

Print release screen showing the jobs awaiting release.

PaperCut Held Print Jobs Refresh Print All Back

Time	Document	Pages	Cost		
11:47:22	Budget – OpenOffice.org Calc	98	\$9.80	Print	Cancel
11:47:21	Microsoft PowerPoint – Presentation	99	\$9.90	Print	Cancel
11:47:20	Microsoft Word – Document1	38	\$3.80	Print	Cancel
11:47:19	research paper.pdf	62	\$6.20	Print	Cancel
11:46:05	Budget – OpenOffice.org Calc	38	\$3.80	Print	Cancel
11:46:04	research paper.pdf	23	\$4.60	Print	Cancel
11:46:03	Microsoft PowerPoint – Presentation	93	\$9.30	Print	Cancel
11:46:02	Stats – OpenOffice.org Writer	25	\$5.00	Print	Cancel

1 / 2 Next >>

User: matt PaperCut MF 11.2.14053

Shared account search / selection screen.

PaperCut Select Account Back

Current selection: Personal account

Search: Search

PIN/Code: Select

myaccount

myaccount\subacct

User: matt PaperCut MF 11.2.14053

User card association

PaperCut Associate New Card

Unknown card, access to device functions is denied. To associate this card with your account, enter your network username and password.

Username:

Password:

PaperCut MF 11.2.14053

13 Appendix E: 08 Code Check list

13.1eBX Codes

Description	08 service code	service mode setting
Card Reader	3500	90001 (e.g. Elatec TWN3) – See Appendix A: Supported Authentication Card Readers
Real-time logging	3623	255
Full logging	3624	4294967295
Populate “To” Address in Scan to Email (optional)	9980	1
Card Authentication LDAP field	9398	eBMUserCard
Extension Label (optional)	9955	PaperCut
Change the “Menu” button to open the EWB directly (optional)	9985	1
Initial default screen be the EWB screen	9132	99
Allow anyone to delete a print job (optional)	8726	1
Allow the user to delete their jobs from the Private/Hold screen on the copier (optional)	9236	3

13.2eB3 Codes

Description	08 service code	service mode setting
Card Reader	1772	90001 (e.g. Elatec TWN3) – See Appendix A: Supported Authentication Card Readers
Real-time logging	3623	255

Full logging	3624	4294967295
Populate "To" Address in Scan to Email (optional)	9980	1
Card Authentication LDAP field	1927	eBMUserCard
Extension Label (optional)	9955	PaperCut
Initial default screen be the EWB screen	331	8

14 Appendix F: TopAccess Settings Check list

14.1eBX TopAccess Settings

Description	Menu
Enable SNMP real-time logs	Administration -> Setup -> Network -> SNMP Network Service
Configure EWB	Administration -> Setup -> EWB
Create LDAP server	Administration -> Maintenance -> Directory Service
Configure RBAC	User Management -> Export/Import -> Import
Enable LDAP authentication in 3 sections: <ul style="list-style-type: none"> 1. User Authentication 2. RBAC 3. Card Authentication 	Administration -> Security
Import Print Data Converter	Administration -> Setup -> Print Data Converter

14.2eB3 TopAccess Settings

Description	Menu
Enable SNMP real-time logs	Administration -> Setup -> Network -> SNMP Network Service
Configure EWB	Administration -> General -> EWB Setting

Create LDAP server	Administration -> Maintenance -> Directory Service
Configure RBAC	User Management-> Role Information -> Export/Import -> Import
Enable LDAP authentication in 3 sections: <ol style="list-style-type: none"> 1. User Authentication 2. RBAC 3. Card Authentication 	User Management -> Authentication -> User Management Setting