PaperCut MF - Toshiba SDK2 Embedded Manual

Contents

1 Document revision history

Published date or release	Details of changes made
19.2.0	2.4.14 Install PaperCut MF
19.0.4	3.1.1. Supported Toshiba Devices
19.0.0	3.2.5 Create Toshiba MFP device in PaperCut; 5.6 SNMP; 5.12 Config Editor
18.1.1	3.2.4.5 Enable the MFP Embedded Web Browser (EWB); 5.1 HTTPS Security (recommended); 5.2 Inbound connections; 6.6 Shared Account Selection; 5.11 Config Editor

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 Which version should I install?

This manual is for Toshiba V2 devices.
To be compatible, devices must support Toshiba Open Platform SDK version 2 or later, and be listed in "2.3.1 Supported Toshiba Devices".
Devices supporting Toshiba SDK 3 or higher should use PaperCut's Toshiba MDS V3 embedded software, documented separately in the manual entitled PaperCut MF - Toshiba MDS V3 Embedded Manual.
Devices that support Open Platform SDK version 2 that had previously been installed with PaperCut's SDK 1 support, can be migrated using the instructions in "1.7 Migrating from SDK 1 to SDK 2 Toshiba Devices".

2.2 Migrating from SDK 1 to SDK 2 Toshiba Devices

SDK Version 2 Toshiba devices in PaperCut have the added feature of Zero Stop when copying as is discussed in section 5.3. If you have a compatible device (see 2.3.1) which is using the non-SDK 2 integration, then some changes are required to take advantage of this. The recommended procedure in converting your PaperCut installation to use an SDK version 2 device includes the following steps:

1. Take the following screenshots from the PaperCut admin interface for the existing Toshiba device:
    a. Summary
    b. Advanced Charging
    c. Filters and Restrictions

These can be used as reference when filling out the new device settings.
2. Delete the existing Toshiba (v1) device.
3. Create a new v2 Toshiba device with the same name as the v1 Toshiba device and use any settings that you noted in the screenshots that are relevant.

NOTE: When the original device is deleted, all historical log records in the PaperCut database will not be deleted. This data will still be available in all the available usage reports.

2.3 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.

- Ensure that your Toshiba MFD is in the list of supported devices. Check the device lists in 2.3.1 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.

2.3.1 Supported Toshiba Devices

Ensure that the devices on the network are Toshiba Open Platform SDK version 2 devices that are listed as supported devices on the PaperCut MF for Toshiba page.

2.3.2 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).
- Outbound connections from PaperCut to the Toshiba Device on ports:
  - 49629 (TCP/HTTP)

2.4 Setup Procedure

This section describes the LDAP and ODCA configuration for these devices.

2.4.1 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 "Administration" tab at the top right of the page.
4. Enter the device administrator username and password, and press "Login". By default this is Admin/123456.

2.4.2 Configuring the 08 “Service Mode” MFP settings

Please note that all 08 “service mode” changes should be done **only by a qualified Toshiba technician**. If many 08 codes need to be set then it is advisable to **not** restart the MFP until all the required settings have been made.

Recent firmware releases of eBX series devices display "Quota Setting" in TopAccess (see the screenshot from section 2.4.12) and do not require the enabling of the 08/6086 code mentioned below. If the "Quota Setting" is not displayed in TopAccess then in order to support the Zero Stop functionality, the Quota Setting should be made accessible by setting the 08/6086 code in the following steps:

1. Enter 08 service mode.
2. Enter: 6086
3. Press the “Start” button.
4. Enter: 1 (0 is the default)
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.

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 code setting is required. See Appendix A: Supported Authentication Card Readers on page 47 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.

NOTE: Recent firmware releases, which shipped with Toshiba e-BRIDGE Next models, do not support the 9398 code. Setup card authentication can be done only from TopAccess. See “Setup Procedure”.

2.4.3 (Optional) Dedicated screen for card authentication

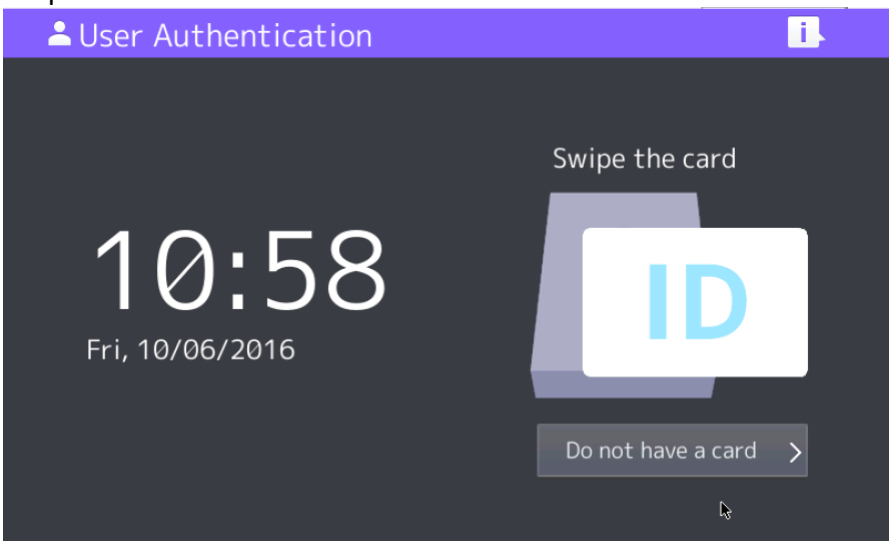
If you want to see a separate screen to prompt for swiping a card then the following 08 code can be used to enable this in the following models and firmware:

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

1. Enter 08 service mode.
2. Check the value of setting 8727, as follows:
    - Enter 8727
    - Confirm that the value is set to either “1” to enable this screen or “0” to disable this screen.
3. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

Swipe Card screen on Toshiba e-BRIDGE Next Series:



2.4.4 (Optional) Change the EXTENSION button label

On Toshiba models previous to e-BRIDGE Next series, 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.
3. Restart the MFP by holding down the “Main Power” button until it stops. Press again to restart.

Note: Recent firmware releases, which shipped with Toshiba e-BRIDGE Next models, do not support the 9955 code. You can now assign the “1” and “2” panel hard keys in TopAccess to point to the EWB URL (Administration -> Setup -> General -> Assignment for Programmable Button)

2.4.5 (Optional) Change the Menu/Extension button to open EWB

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.

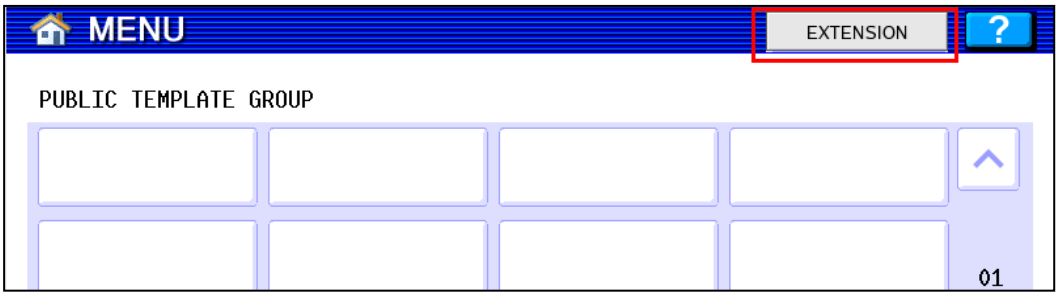
Note: Recent firmware releases, which shipped with Toshiba e-BRIDGE Next models, do not support the 9985 code. You can now assign the “1” and “2” panel hard keys in TopAccess to point to the EWB URL.

2.4.6 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 (on Toshiba models previous to e-BRIDGE Next series):

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. Note that his button may have been re-labeled in section 2.4.4.



To configure the EWB:

1. Log in to the MFP web interface (TopAccess) with your web browser.
2. Log in as the “Admin” user and select the “Administration” tab.
3. Navigate to the “Administration” -> “EWB” page.
4. Under the “Home Page Setting” set the “Home Page” setting as below:

http://server-address:9191/device/toshiba/
changing “server-address” for the address of your PaperCut server.

5. Alternatively, if using an encrypted HTTPS connection, then use:
   https://server-address:9192/device/toshiba/
   where “server-address” is the server’s fully qualified domain name.
   For more information about using an encrypted HTTPS connection, see 4.1 HTTPS Security (recommended).
6. Press the “Save” button.

2.4.7 Enable the Server Registration Setting

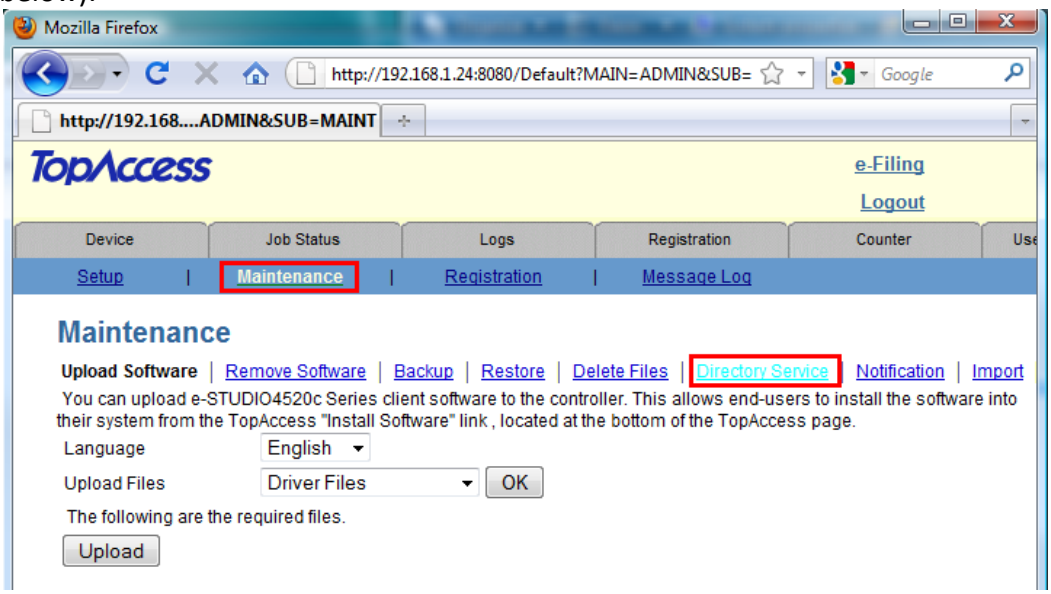
In order to enable the Job Status button on the Held Jobs page, the Application Server address must be added to the Server Registration Setting.

1. Log in to the MFP web interface (TopAccess) with your web browser.
2. Log in as the “Admin” user and select the “Administration” tab.
3. Navigate to the “Administration” -> “EWB” page.
4. Under the “Server Registration Setting”, click on the "Add" button and add the following server address (changing “server-address” for the address of your PaperCut server):
   http://server-address:9191/
5. If the EWB address above is using "https" then please add:
   https://server-address:9192/

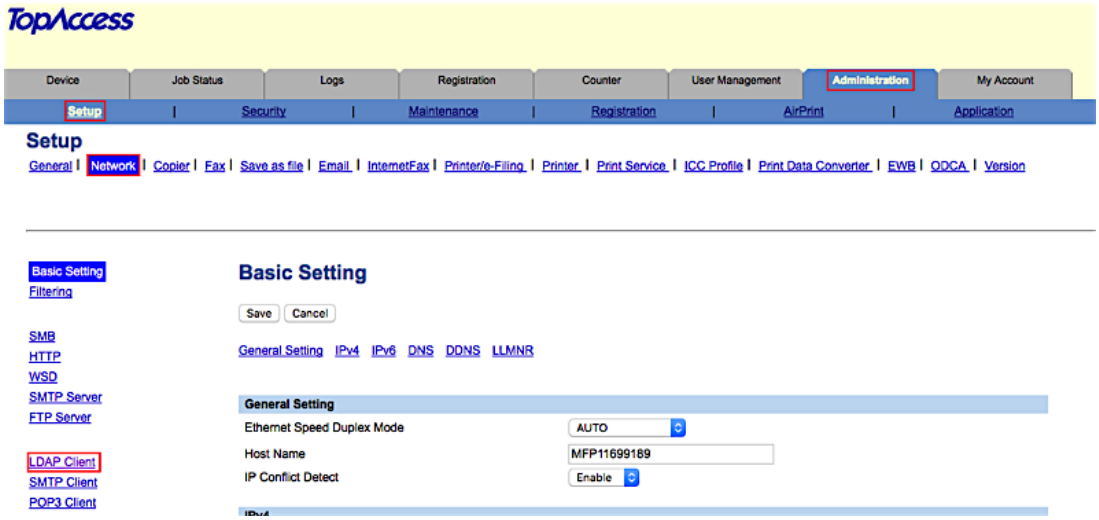
2.4.8 Configure MFP LDAP server

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:

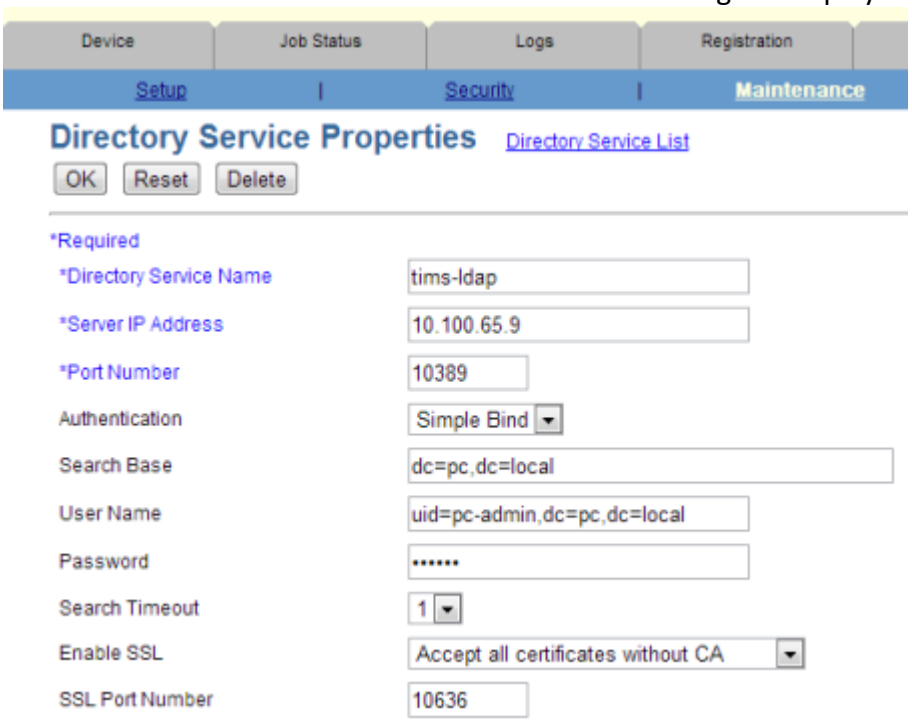
1. Log in to the device’s web administration (TopAccess) with a web browser as an admin user.
2. Select the “Administration” tab
3. Select the “Maintenance” sub-section, and the “Directory Service” option (see below).



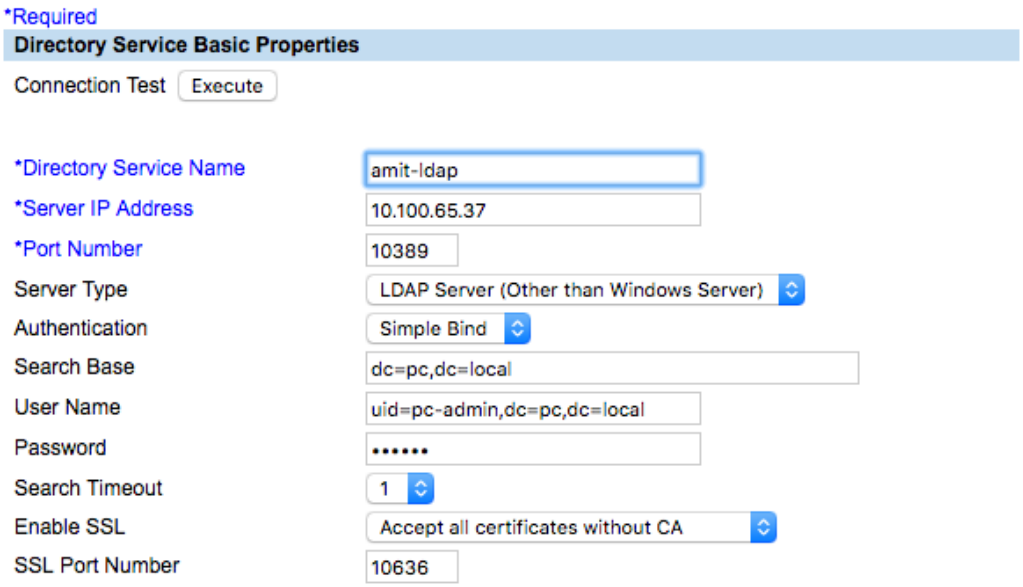
NOTE: On Toshiba e-BRIDGE Next series, Configuring LDAP server has been moved to: Administration -> Setup -> Network -> LDAP Client (see screenshot below).



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



NOTE: On Toshiba e-BRIDGE Next series, new field appears: “Server Type”. See the table below.



Directory Service Name	Any name to identify the PaperCut LDAP server.
Server IP address	The network address of the PaperCut server.
Port	10389
Server Type	LDAP Server (Other than Windows Server)
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”/”Save” to save the LDAP settings.
6. If you have multiple LDAP servers defined, select the newly created LDAP server as the default.

2.4.9 (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.

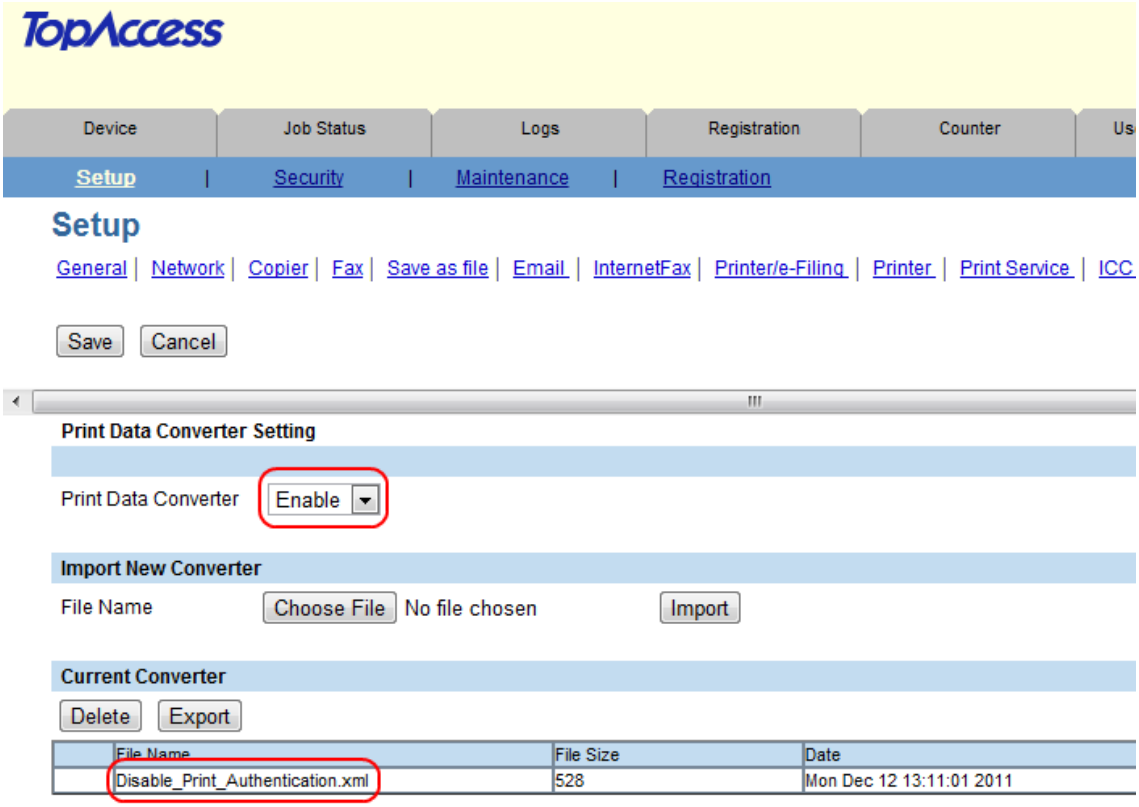
Note that if you change the LDAPS port to another number, then you must restart the PaperCut Application Server (to make it listen on the new port) and you must make sure that your server’s firewall is not blocking this port number.

2.4.10 Configure Print Data Converter

To ensure that the Toshiba MFP does not attempt to track print jobs or restrict them in any manner, you need to install a Print Data Converter file.
To import a Print Data Converter file:

1. Log in to the device web administration (TopAccess) with a web browser.
2. Select the “Administration” tab and “Setup”.
3. Select the “Print Data Converter” link.
4. In the “Import New Converter” section, “Choose” the following file located on the PaperCut server installation:
   `[app-path]\providers\hardware\toshiba\Disable_Print_Authentication.xml`
5. Press the “Import” button.
6. Enable the Print Data Converter from the drop-down list.

7. After completing this import the screen should look like the following:



One caveat with doing this is that 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:

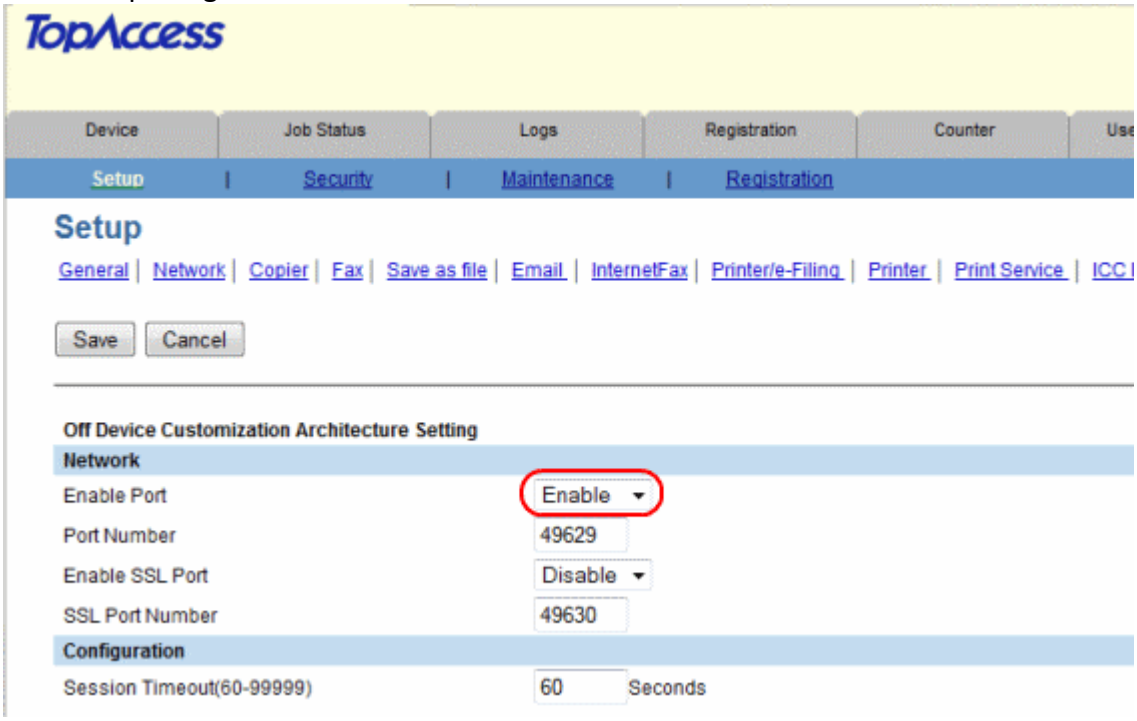
1. Enter 08 service mode.
2. Change setting 9236 to 3 (default is 1). To do this:
    a. Enter: 9236
    b. Press "Start" button
    c. Enter: 3 (to allow users to see their own jobs and be able to delete them)
    d. Press the "OK" button on the LCD screen.

2.4.11 Enable ODCA (Off Device Customization Architecture) Setting

To support the communication of a variety of tasks in SDK2, the ODCA setting should be enabled.

1. Log in to the device web administration (TopAccess) with a web browser.
2. Select the "Administration" tab and "Setup".
3. Select the "ODCA" tab.
4. Enable the port in the drop down list.

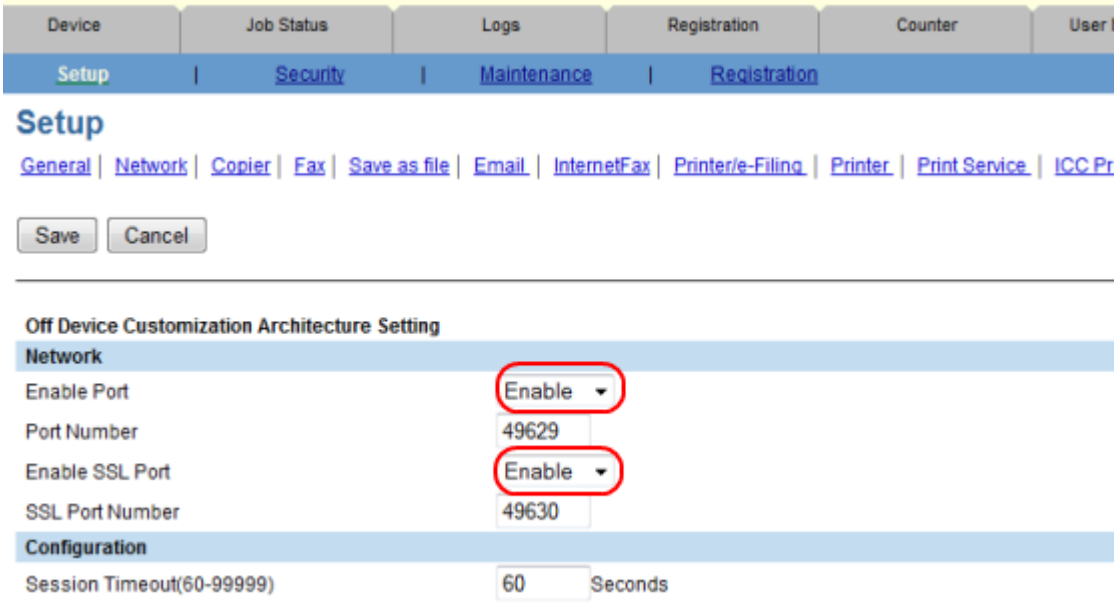
5. After completing this the screen should look like this:



2.4.11.1 Enable Secure ODCA

By enabling secure ODCA, the SDK2 calls such as getting the Toshiba log information for tracking of the users' copies/faxes/scans, will be encrypted.

1. Choose "Enable" for the "Enable SSL Port" field.
2. Set the Toshiba Device Advance Configuration parameter of ext-device.toshiba.v2.secure-odca to "Y".
3. After completing this the screen should look like this:

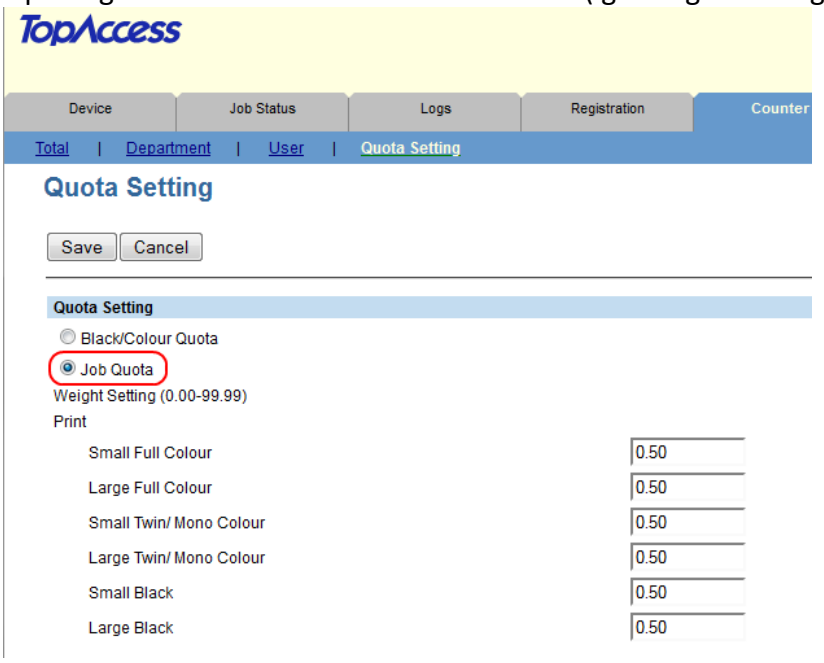


4. **NOTE**: If the Toshiba Device Advance Configuration parameter of *ext-device.toshiba.v2.port-num* is set to "49629" then it should be changed to either "49630" or "DEFAULT".

2.4.12 Enable Job Quota for Zero Stop

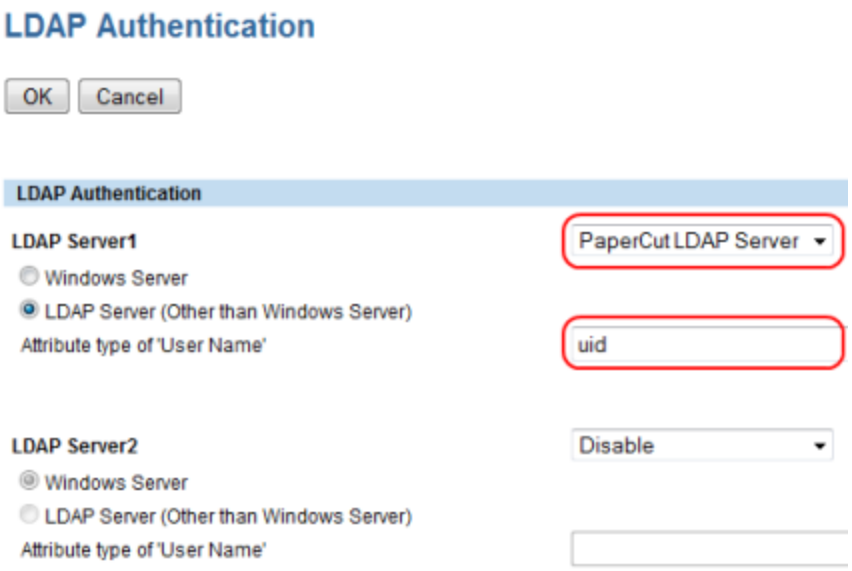
To enable the zero stop functionality, the Quota Setting needs to be set to “Job Quota”. Please ensure that the corresponding 08 code is set in section 2.4.2.

1. Log in to the device web administration (TopAccess) with a web browser.
2. Select the “Counter” tab.
3. Select the “Quota Setting” tab.
4. Select the “Job Quota” for the Quota Setting (instead of the default of “Black/Colour Quota”).
5. Please disregard the Weight Setting values as they are irrelevant.
6. After completing this the screen should look like this (ignoring the Weight Setting values):

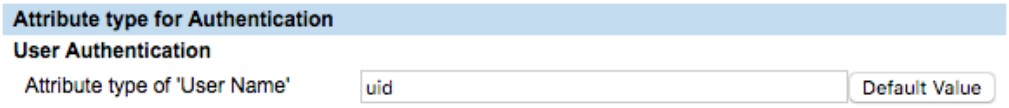


2.4.13 Enable LDAP User Authentication

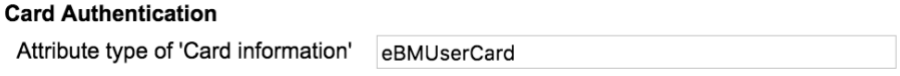
1. Log in to the device’s web administration (TopAccess) with a web browser.
2. In TopAccess, select “Administration” -> “Security”.
3. Under the “User Authentication Setting” heading change the following options.
4. Change “User Authentication” to “Enable”.
5. Change “Authentication failed print job/Raw 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.



10. Set the "Attribute type of 'user name'" to **uid**. (Please note that this is case-sensitive.)
    NOTE: For the Toshiba e-BRIDGE Next series, set the 'User Name' attribute type on the LDAP Client screen, (see 2.4.8). Click on an existing Server Entry. The Edit LDAP Information popup is displayed. Set the 'User Name' attribute to **uid**.

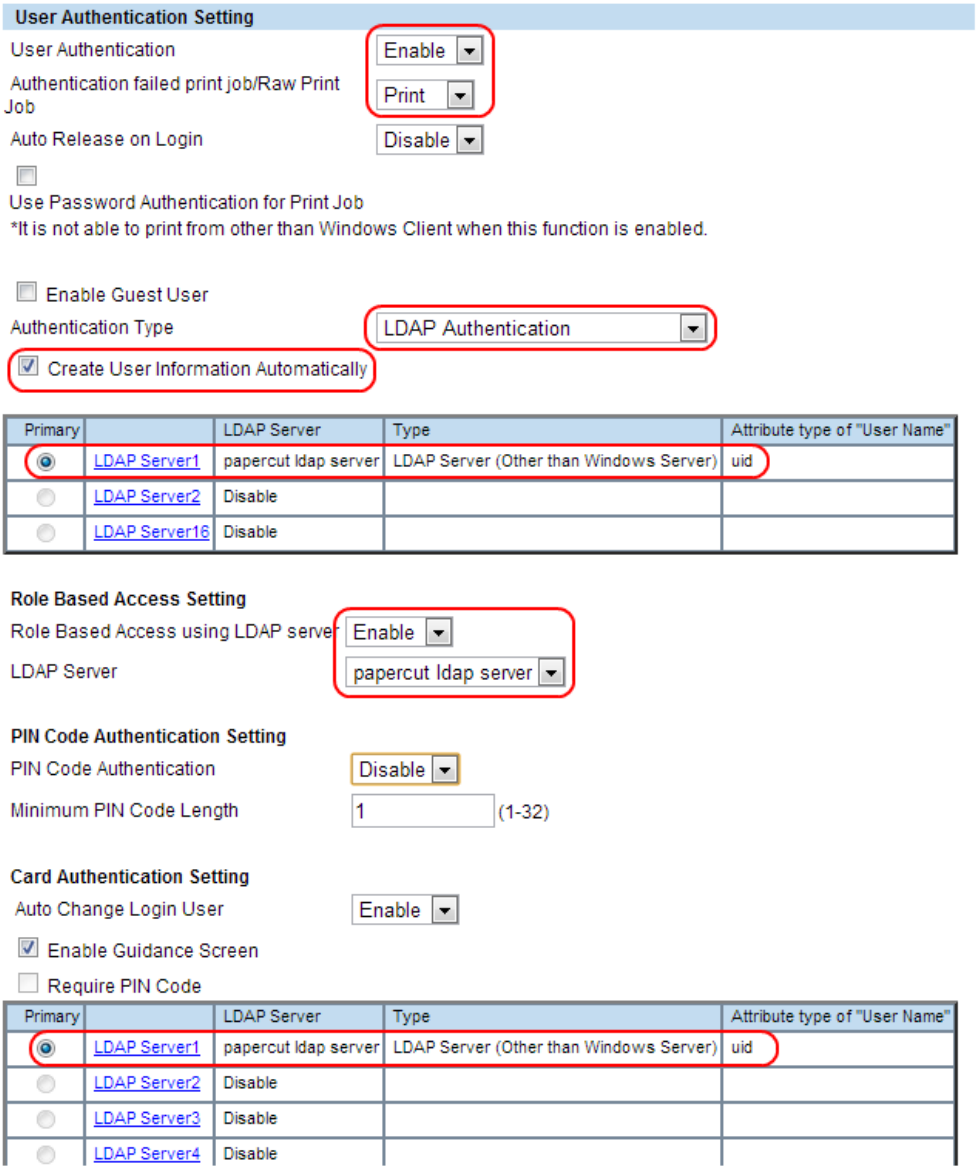


11. Press "OK"/"Save"
12. Enable the RBAC by setting "Role Based Access using LDAP server" to "Enable".
13. Set the RBAC LDAP server to the PaperCut LDAP server defined previously.
14. If using card authentication, set the card authentication LDAP Server to the PaperCut LDAP server previously defined.
    NOTE: On Toshiba e-BRIDGE Next series, setting the attribute type for card authentication can't be done using a service mode (used to be 9398). Instead, in "LDAP Client" there is a new 'Card Authentication' section with "Attribute type of 'Card Information'" attribute. Set it to **eBMUserCard**:



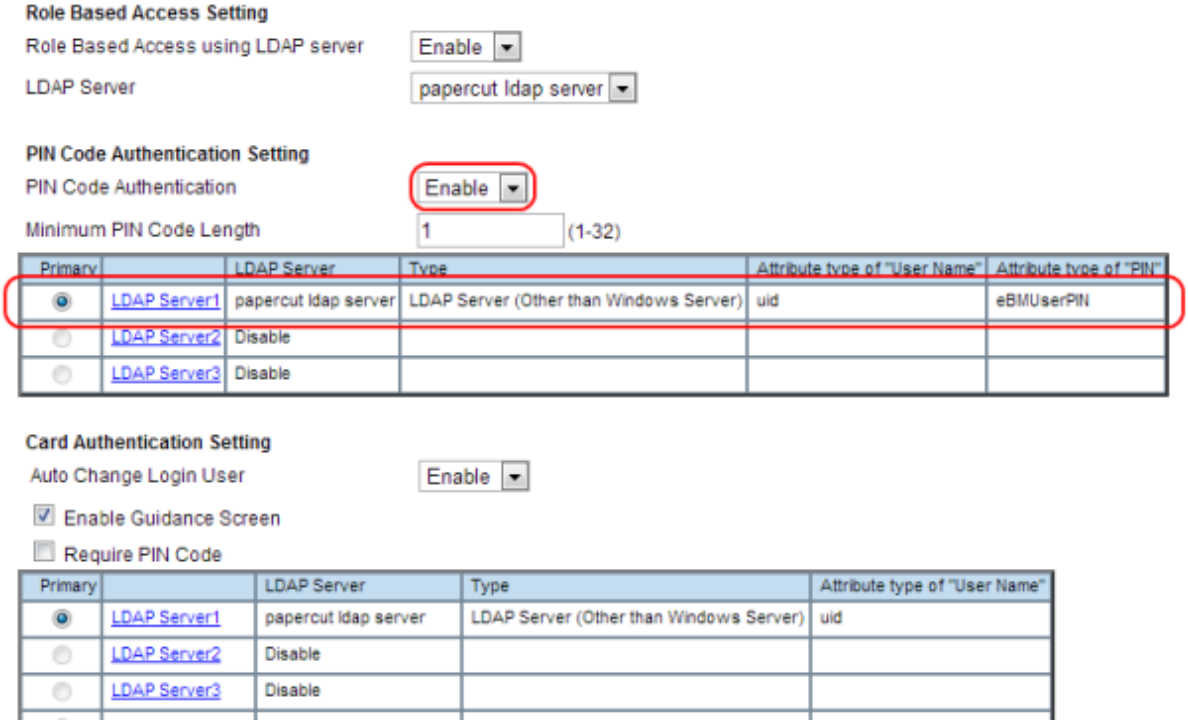
15. Please check that the PaperCut LDAP server is specified now in 3 places:
    1. User authentication
    2. Role based access setting
    3. Card authentication setting
16. If under "User Authentication Setting" it has the option of "Create User Information Automatically", ensure it is enabled.
17. 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").

18. Verify that the settings are all set as described (see screenshot)

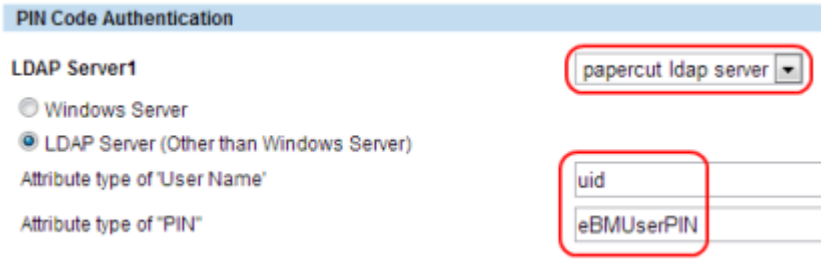


19. If the MFP supports PIN authentication, you have PaperCut MF version 13 or higher and you want to support Identity Number authentication in PaperCut, then you

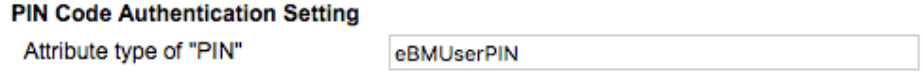
should enable PIN Code authentication.



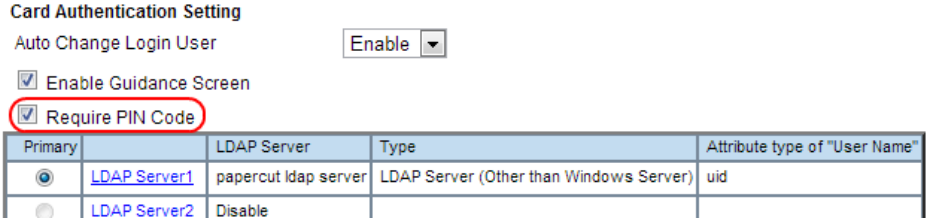
20. Set the “Attribute type of ‘User Name’” to **uid**.
21. Set the “Attribute type of ‘PIN’” to **eBMUserPIN**.



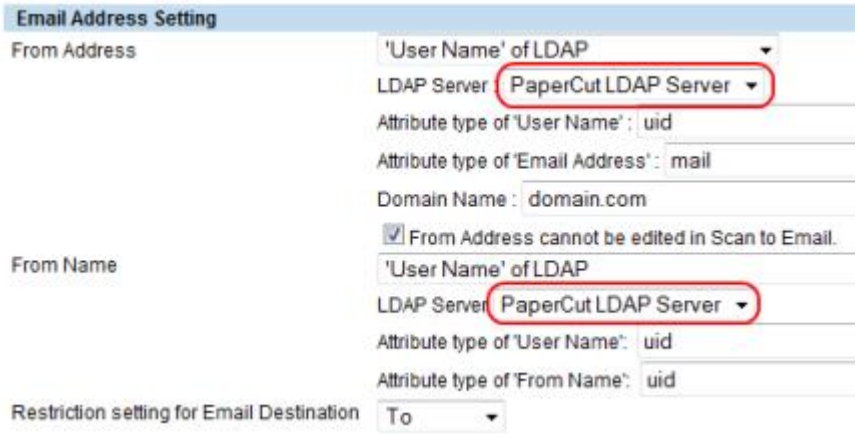
NOTE: on Toshiba e-BRIDGE Next series, setting up the Attribute type of ‘PIN’ is done in “LDAP Client” screen (see 2.2.4.7). Go to an existing Server Entry and click on it. A popup titled “Edit LDAP Information” will appear. Set the ‘PIN’ attribute to **eBMUserPIN**.



22. If you have PaperCut MF version 13.1 or higher and you want to support swipe cards requiring a PIN, then enable “Require PIN Code” for the Card Authentication Setting.



23. Optionally, you can set up the Email Address Setting. An example setting is:



When User Authentication or Email Authentication is enabled, select whether to set the Email address of the authenticated user as a destination. The available options are (we have chosen the “To:” option in the screenshot):

Option	Purpose
None	Not used as a destination
Fixed To	Only the Email address of the authenticated user is used for "To".
To	The Email address of the authenticated user is added to "To".
Cc	The Email address of the authenticated user is added to "Cc".
Bcc	The Email address of the authenticated user is added to "Bcc".

24. Press “Save” to confirm the changes.
25. Reboot the MFP for these settings to take effect.

2.4.14 Install PaperCut MF

To enable communication between the PaperCut MF Application Server and the devices that have been installed with the PaperCut MF embedded application:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to Options > Advanced.
3. In the External Hardware Integration area, select Enable external hardware integration (for supported devices only).
4. Click Apply.
5. You can use any one of the following options:
    - 2.4.14.1 Install PaperCut MF on multiple devices
    - 2.4.14.2 Install PaperCut MF on each device

2.4.14.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 introduced a feature to create multiple devices in bulk through a CSV file via server commands. In 20.0.0 we added a way to load this CSV file via the PaperCut MF UI. You can find the feature under: PaperCut MF > Devices > Create multiple devices. Using this feature increases your operational efficiency by significantly reducing the time taken to add devices to PaperCut MF. From version 20.0, this feature also allows for you to add devices to PaperCut MF before such devices are delivered to their installation site, such devices are added with a "Staged" status. The scenario for "Staged" devices applies when the system admin already knows all the device's attributes prior to its delivery. For more information, see the Enhanced Deployment Project.

2.4.14.2 Install PaperCut MF on each device

Note: If you are running a version prior to PaperCut MF 19.2.0, then this is the only applicable option.

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Select the "Devices" tab.
3. Create device" action link on the left.
4. Choose Device type of "Toshiba v2".
5. Enter the device details, including the network address / IP address of the Toshiba device.
6. Select the device functions to control/log (e.g. copying, scan, fax, etc).
7. Press OK, to create the device.
8. 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.
9. Press "OK" to save the changes.
10. The device appears on the device list. If the connection to the device is established the status column will not have an "error" state.

Device Name ▲	Function	Type	Hostname	Status
device\Library Copier	Fax, Copier, Scanner	Toshiba v2	192.168.1.28	Started

2.5 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).

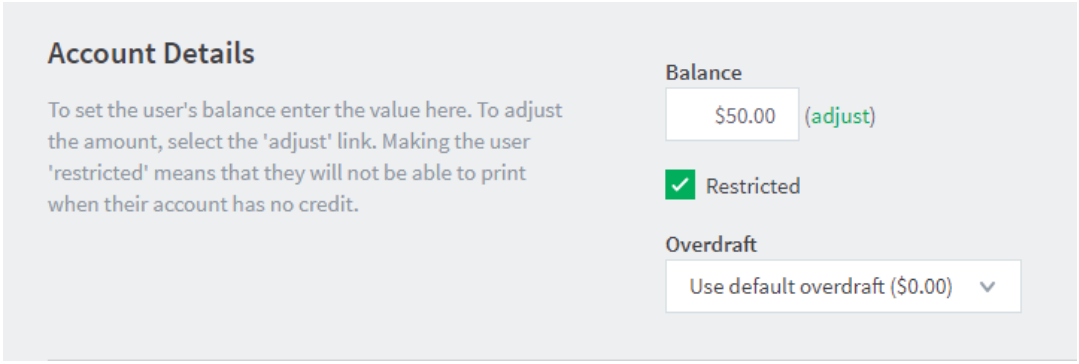
If you already have existing users for testing, then there is no need to create the users above. Instead you can use your existing users for testing.

To setup these users in PaperCut:

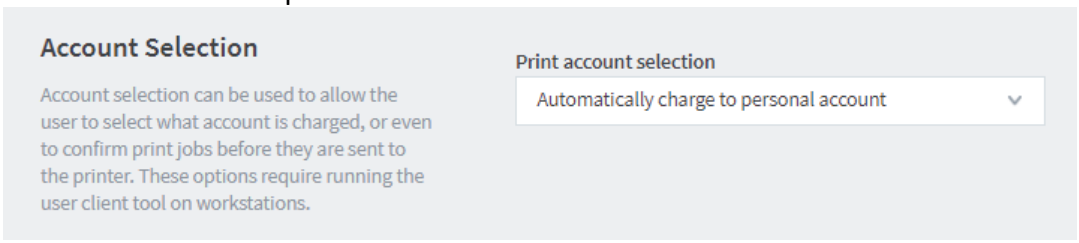
1. Create the 'testusersimple' and 'testuseradvanced' users in your Active Directory or LDAP directory.
2. Login to the PaperCut's admin web interface
3. Go to the "Options->User/Group sync" page and press "Synchronize Now".
4. Once the sync is complete, the users will be added to PaperCut.

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".



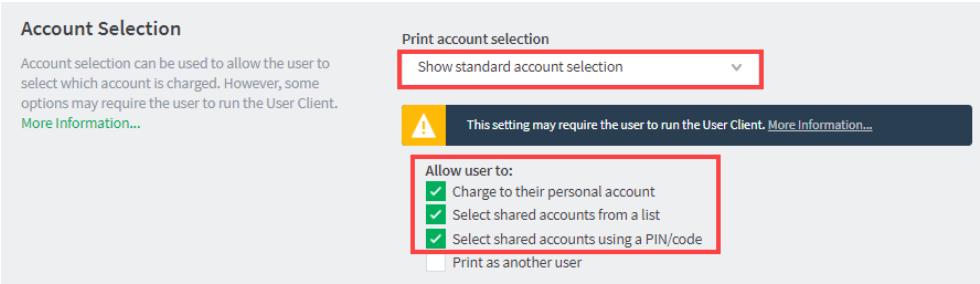
4. Verify that this user is set to "Automatically charge to personal account" in the "Account selection" options.



5. Press the "OK" button to save.

To configure 'testuseradvanced':

1. In PaperCut, select the "Users" tab
2. Select the 'testuseradvanced'user.
3. Change the "Account Selection" option to "Show standard account selection" and enable the relevant account selection options.



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.

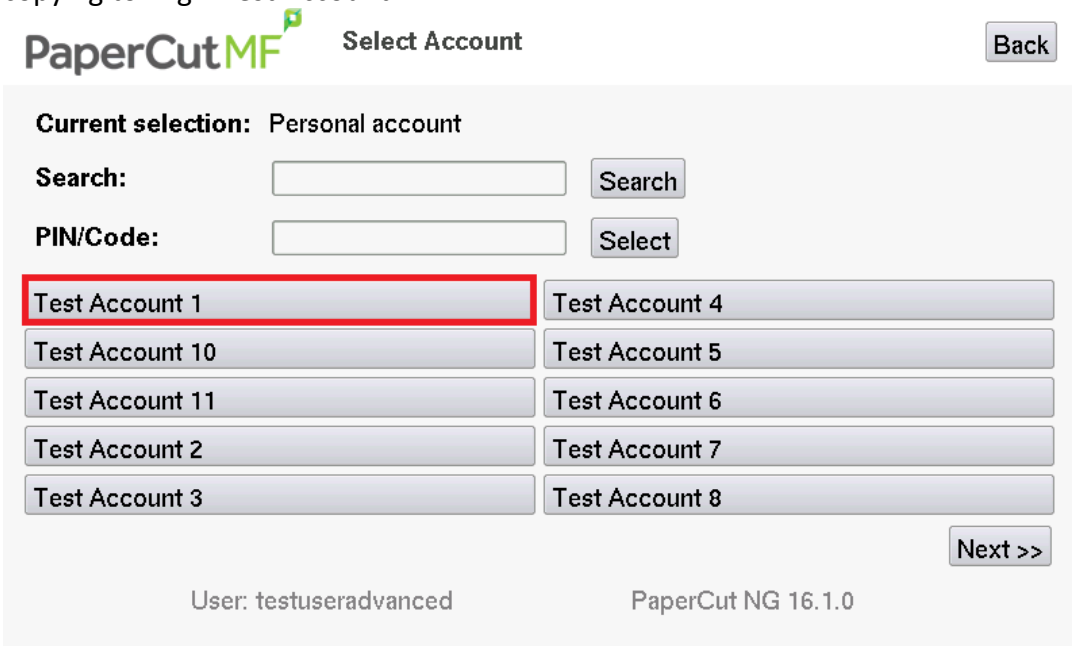
First some test accounts should be created:

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:

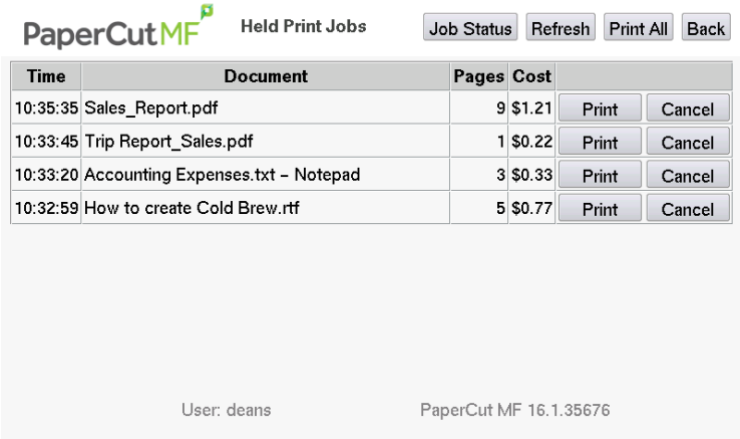
1. In PaperCut, select the “Printers” tab.
2. Select the print queue (i.e. not the ‘device’) for the Toshiba MFD that is used for testing.
3. Enable the “Hold/release queue” option.
4. Press OK/Apply to save the changes. All printing to this queue will now be held until released by a user.

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.



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.

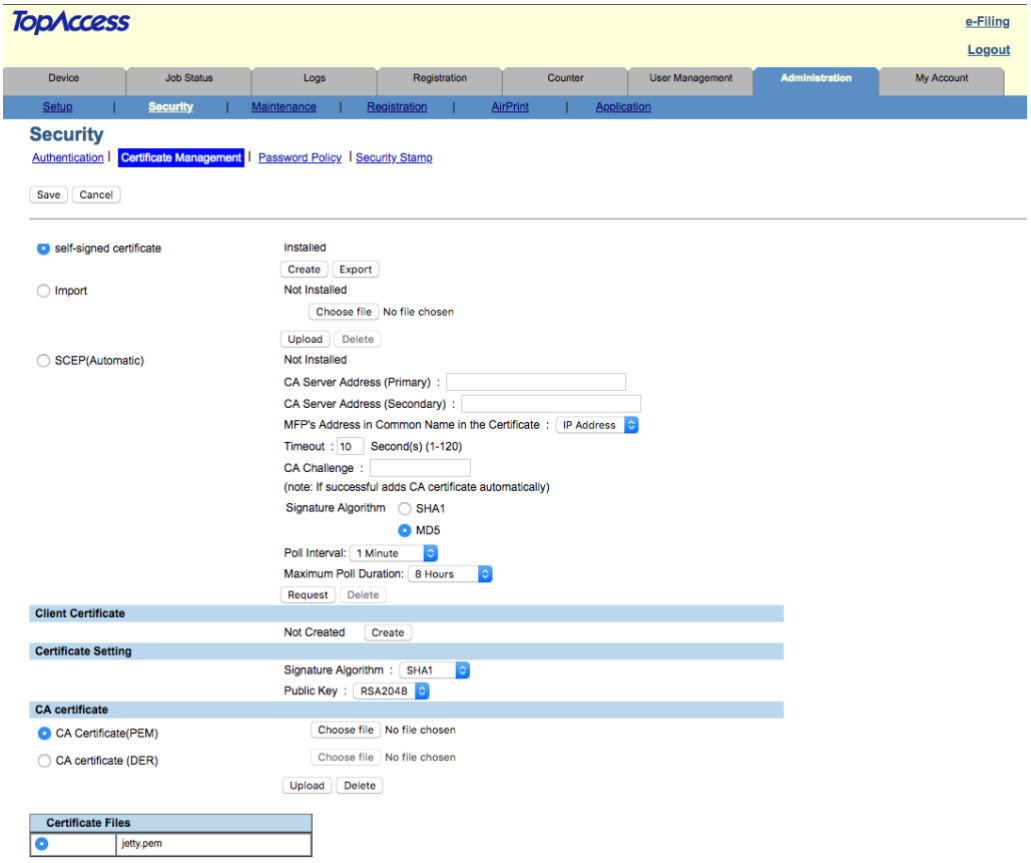
4 Configuration

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 HTTPS Security (recommended)

PaperCut MF can be configured to communicate with the device using the HTTPS (SSL/TLS) protocol, which is a secure and encrypted protocol.
To enable HTTPS:

1. You must have an SSL certificate installed on the PaperCut MF Application Server. The certificate must use the server's fully-qualified domain name. This must be defined either in the **Common Name** (CN) field or included in the **Alternative Names** (AN) of the subject of the certificate. Without this, the device cannot connect to the server, since devices do not work with hostname-only certificates (i.e. not fully qualified).
   You may use an official Certificate Authority-signed certificate or a self-signed certificate:
   - If you are using an official CA-signed certificate (for example, Verisign, Thawte), it is likely to use the server's fully qualified domain name (or wildcard). This is because Certificate Authorities generally no longer accept certificate requests for either intranet names or IP addresses.
   - If you are using the self-signed certificate that is generated by default when installing PaperCut MF, ensure to regenerate it for a fully qualified domain name. This is because the default self-signed certificate generated during PaperCut MF installation (device registration and integration) is issued using a hostname, instead of the domain name. Regenerate it using PaperCut MF's `create-ssl-keystore` tool in:
     `[PaperCut MF Install Location]\server\bin\[platform]`
     Run the following command to regenerate the certificate using the tool:
     `create-ssl-keystore -f "myserver.fullname.com"`
     For more information, see the PaperCut MF manual.
     After the certificate is regenerated, you must upload it on the device's web interface (TOPACCESS). To upload the regenerated certificate on the device's web interface (TOPACCESS):
     a. Extract the regenerated certificate that is installed on the PaperCut MF Application Server, using Keystore Explorer (the password is *default*), as a PEM file. For more information, see SSL with PaperCut and Keystore Explorer.
     b. Log in to the device's web interface (TOPACCESS) as an administrator.
     c. Navigate to **Administration > Security > Certificate Management**
     d. In the **CA Certificate** section, select **CA Certificate (PEM).**
     e. Click **Choose file** and follow the prompts to upload the extracted regenerated certificate (PEM file):



f. Click **Save**.

2. Use the following config keys:
   ext-device.toshiba.v2.secure-odca
   ext-device.toshiba.v2.secure-app-server-url
   system.network-address
   For more information, see 4.12 Config Editor.
3. Ensure to configure the EWB to use an encrypted HTTPS connection by setting the server address with its fully qualified domain name. For more information, see 2.4.6 Enable the MFP Embedded Web Browser (EWB).
4. Ensure to enable secure ODCA. For more information, see 2.4.11 Enable ODCA (Off Device Customization Architecture) Setting.
5. Ensure to configure inbound connections to PaperCut MF Application Server. For more information, see 4.2.1 Inbound connections to PaperCut MF Application Server.

4.2 Inbound connections

4.2.1 Inbound connections to PaperCut MF Application Server

To configure PaperCut MF to allow inbound connections from the device to the PaperCut MF Application Server, use the config key **system.network-address**. For more information, see 4.12 Config Editor.

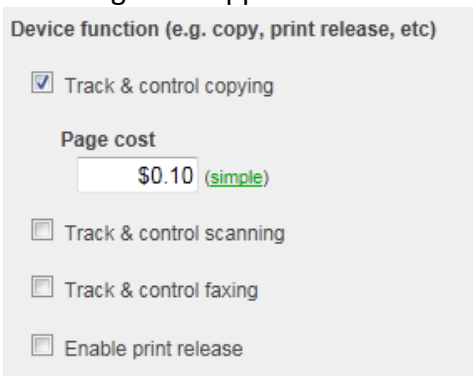
4.2.2 Inbound connections to PaperCut MF Site Servers

To configure PaperCut MF to allow inbound connections from the device to PaperCut MF Site Servers on the PaperCut MF Admin web interface:

1. Site Servers must already be installed and configured. For more information, see the PaperCut MF manual.
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Sites**.
4. Select the Site Server.
5. In the **Configuration** area, enter the network IP address (if using HTTP) or DNS name (if using HTTP or HTTPS) of the PaperCut MF Site Server that the device uses to make inbound connections.
6. Click **Apply**.

4.3 Device Function

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



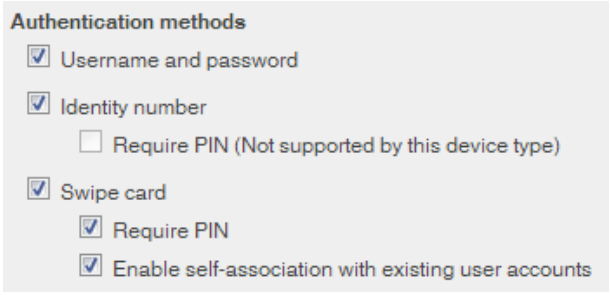
Each device function is discussed in the following table.

Device Function	Description
Track & control copying	The device will track walk-up off-the-glass copying 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.

4.4 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 available for a device

Each authentication method is discussed in the following table.

Authentication Method	Description
Username and password	The user may use their domain/network username and password to log into the device.
Identity number	The user can enter a predetermined number to log into the device. The dialog on the panel will actually ask for a PIN but this is actually referring to PaperCut's identity number associated for that user. This method is supported since PaperCut MF version 13.
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->Require PIN	The user may log in by swiping a card and then entering a PIN in the dialog on the MFC panel. This requires a PIN to already be assigned to the user – they will not be prompted for a PIN if one has not been set for the user. This method is supported since PaperCut MF version 13.1.
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. If PIN support is enabled on the MFC, then the user will need to enter "0" when prompted for the PIN.

Description of authentication methods

4.5 Account Selection

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 to select an account to charge a job to, is based on the following configurations:

- Account Selection options configured for users on the PaperCut MF Admin web interface (**Users > User List > User Details > Account Selection**). For more information, see the PaperCut MF Manual.
- Shared Account access configured for users on the PaperCut MF Admin web interface (**Accounts > Shared Accounts List > Account Details > Security**). For more information, see the PaperCut MF Manual.

4.6 SNMP

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.

By default, PaperCut MF uses SNMPv1/v2c to perform these actions. You can, however, select to use SMPv3 for better security and encryption. For more information about SNMP, see the PaperCut MF manual.

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, Username, Privacy password, Authentication password** - If these values are available at the device's web interface, then use the same values. It 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.**

4.7 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.

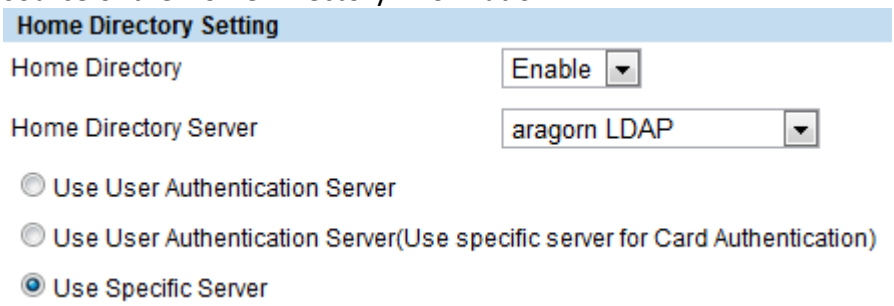
The text can be customized by editing the device configuration from the PaperCut administration interface. For more details see the Advanced Configuration section.

4.8 Setup Scan-to-Network Folder

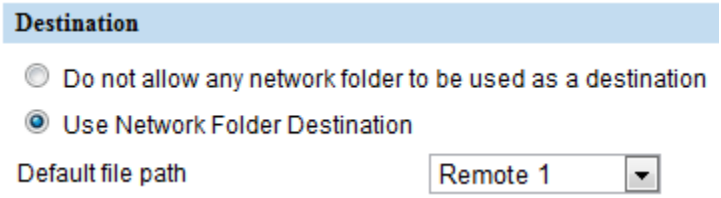
Toshiba devices can be configured to scan to network folders that can be predetermined for each user. This functionality **requires** PaperCut MF version 12.4 or later. The process to configure this functionality is:

1. Under the Toshiba TopAccess configuration, navigate to Administration -> Security.
    a. Click the LDAP Server link that is set as the Primary for Role Based Access Setting.
    b. In the new window, set the "Attribute type of 'User Name'" to "sAMAccountName" instead of "uid".
    c. Repeat this process, if necessary, for the Primary LDAP Server for Card Authentication Setting.
    d. When the settings have been completed as indicated above, click Save.
2. Create a directory server connection under the Toshiba TopAccess configuration, navigating to Administration -> Maintenance -> Directory Service
   NOTE: Toshiba e-BRIDGE Next series has moved the Directory Service menu to a different location. For further information, please consult your Toshiba support.
   Click "New" and fill out the LDAP settings with details that point to the AD/LDAP directory containing the users' network folder information.
3. Under the Toshiba TopAccess configuration, navigate to Administration -> Security and locate the **Home Directory Setting** section.

    a. Set the option to "Enable".
    b. Select the directory server object created in Step 1.
    c. Select the option "Use specific server", to choose the server in Step 2b as the source of the Home Directory information.



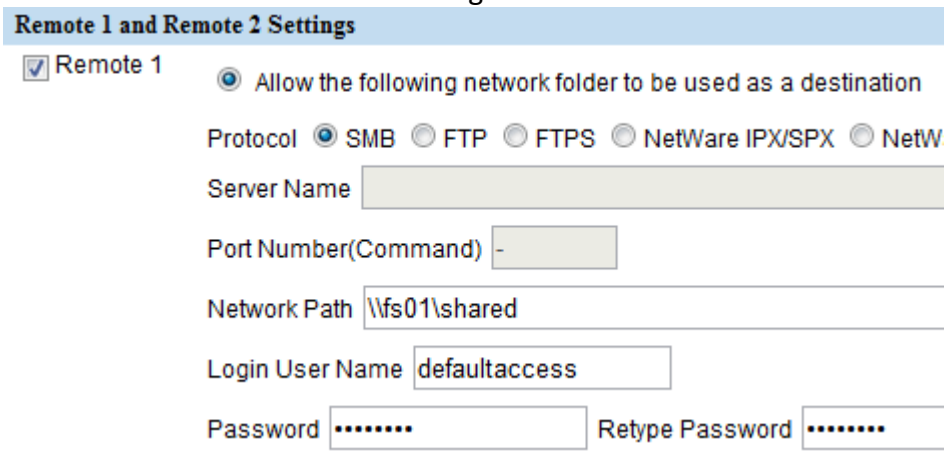
    d. When the settings have been filled out as indicated above, click Save.
4. Under the Toshiba TopAccess configuration, navigate to Administration -> Setup -> Save As File, and locate **Destination.** Select "Use Network Folder Destination", and set the "Default File Path" to "Remote 1".



5. On the same screen, locate the **Remote 1 and Remote 2 Settings**.
    a. Fill out the settings under "Remote 1". This is the network location that will be overwritten by the user's home directory attribute. The entered details

will be used as the default if the user's home directory cannot be queried from the directory server object used in Step 1 and 2.

b. Enter the login username/password for a user account that has **read/write permissions to all user home directories**. These credentials will be used to authenticate to the shared drive if the user authenticates with card authentication. If the user logs into the device with standard credentials, those will be used to authenticate against the network folder.



6. When the settings have been filled out as indicated above, click Save.

4.9 Adding application button links on the welcome page

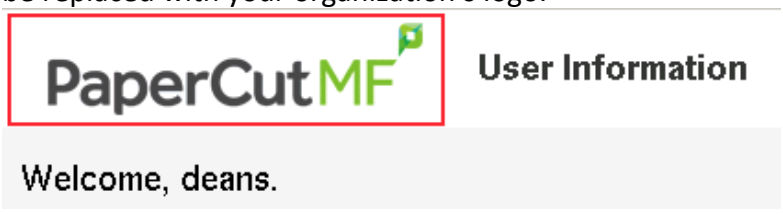
PaperCut allows one or two buttons to be added to the intial PaperCut welcome page which allows the Embedded Web Browser (EWB) to redirect to configured URLs. This can be used, for instance, to go to a 3rd party scan connector application. For more details about the configuration variables to set, please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

4.10Customizing 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.

4.10.1 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

4.10.2 Custom Header Color

The header colors are defined in the Advanced Config settings as described in Section 4.12. 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).

4.11Configuring 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*`

4.12Config 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.admin.password	The admin password for the Toshiba copier.
ext-device.admin.username	The admin username for the copier, by default it is “admin”.
ext-device.card-no-regex	See chapter section 4.11.
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.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.toshiba.release-columns	The columns to display in the print release screen. This is a comma separated list of column names. The valid column names are: • time – the time of the job • user – the username of the user that printed • document – the document name • pages – the number of pages in the job • cost – the cost of the job • client – the client machine name • datetime – the date & time of job When set to DEFAULT the following are used: Secure print release mode: time, document, pages, cost. Release any mode: time, user, document, pages, cost

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 *N* 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 *Letter* and elsewhere it is *A4*.
ext-device.toshiba.v2.limit-reference.quota.duplex	Whether we consider the page to be duplex for the page quota. By default, we consider the page to be duplex so we don't overcharge the user.
ext-device.toshiba.v2.limit-reference.quota.large-paper-size	The reference paper size that we consider to be a large paper size for the zero stop page costs. By default, for the United States this size is *Ledger* and elsewhere it is *A3*.
ext-device.toshiba.v2.limit-reference.quota.small-paper-size	The reference paper size that we consider to be a small paper size for the zero stop page costs. By default, for the United States this size is *Letter* and elsewhere it is *A4*.
ext-device.toshiba.v2.log-highest-id	The highest log id that we have processed so far. Used to determine what log entries to look at next from the copier. If the device's hard disk drive has been erased or replaced, it might stop sending copy job logs to PaperCut. To prevent this from happening, set this value to -1 after erasing the drive.

ext-device.toshiba.v2.port-num	The port number used for ODCA (Off Device Customization Architecture) as set up in TopAccess, as discussed in section 2.4.11.
ext-device.toshiba.v2.serial-number	The serial number of the device that we last queried from the device. This is used so that we know if the device changes across restarts of the PaperCut application server.
ext-device.toshiba.v2.zero-quota-logout	When set to "Y" always reset the user's quota on the MFP is set to zero at logout. Default: "N" When a user logs into the MFP, there is a slight delay until the quota/balance is set **on the MFP**. Until it is set the user's quota from their previous MFP login is used. If their previous quota/balance was zero, they may see a "quota exceeded" message briefly before the quota is set. Setting this to "N" (the default) will not zero the quota on user logout. This means that if the user can login and access the copier before the quota is set that may be able to use the device with their old quota (that may be out of date). Setting this to "Y" will zero the user's quota on each logout. This provides stricter enforcement, but with the possible downside that users can login and access the copier before the quota is set and they will see the "Quota exceeded" message.
ext-device.toshiba.v2.set-roles	When set to "N" it will prevent PaperCut from automatically setting the data for the RBAC (Roles Based Access Controls) allowing the admin to manually set the data. Default: "Y" (will set the RBAC data every 12 hours to ensure it is still correct)
system.network-address	Specify the network IP address (if using HTTP) or DNS name (if using HTTP or HTTPS) of the PaperCut MF Application Server that the device uses to make inbound connections. This is a global config key. • Values: Network IP address (if using HTTP) or DNS name (if using HTTP or HTTPS) of the PaperCut MF

	Application Server used by the device for inbound connections **Note:** For more information, see 4.2.1 Inbound connections to PaperCut MF Application Server and 4.1 HTTPS Security (recommended).
ext-device.toshiba.v2.secure-app-server-url	When set to “Y”, the MFP will use SSL for for login/logout and job completion events sent to the PaperCut server. These events typically include minimal user data and in most cases SSL would not be required. Default: “N” (Events will not be encrypted). For more information, see 4.1 HTTPS Security (recommended).
ext-device.toshiba.v2.secure-odca	When set to “Y”, PaperCut will use SSL for the SOAP communications with ODCA. This will ensure the setting of quotas and the Toshiba log information will be encrypted. Default: “N” (ODCA messages will not be encrypted) For more information, see 4.1 HTTPS Security (recommended)
ext-device.toshiba.v2.overrun-offset	Used to reduce the chance of the overrun of zero stop causing the balance to go negative. It works by submitting to the MFP for its quota, the balance of the account minus the overrun offset. For example, if the account had $2 and the overrun-offset was $0.20 then the MFP would be told the account has a balance of $1.80 in order to make sure it stops printing earlier to avoid overrun. NOTE: The problem with modifying this setting is that it can then prevent the user from doing any printing when they reach below that threshold. For example, if this amount is set to $0.20, and they have enough money to print a $0.10 job, then they will be denied (which may not be expected by the user). Do **not** change this setting unless you understand the repercussions. Default: “0” (Do not subtract anything from the account balance sent to the MFP)

ext-device.toshiba.v2.login-credit-check	When set to "Y" it will always do a credit check at login time to decide whether to allow the user copier access. If set to "N", then PaperCut will rely on the zero-stop mechanism on the device to prevent doing a copier function without enough credit. Since zero-stop is not supported for Faxing, having this configuration enabled may be useful to prevent users from faxing without enough credit. Default: N (don't do credit check on login; rely on zero-stop)
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	OPTIONAL: The application label for the 1st button (if needed). Default: NONE (the button will not be displayed if this is set to “NONE”)
ext-device.toshiba.app-button1.url	OPTIONAL: The application URL for the 1st button (if needed). Default: NONE (need to change to a valid URL if you want to use this button)
ext-device.toshiba.app-button2.label	OPTIONAL: The application label for the 2nd button (if needed). Default: NONE (the button will not be displayed if this is set to “NONE”)

ext-device.toshiba.app-button2.url	OPTIONAL: The application URL for the 2nd button (if needed). Default: NONE (need to change to a valid URL if you want to use this button)
ext-device.block-release-on-error.snmp-error-list	Specify the errors that will prevent jobs from being released. This is a global config key. • DEFAULT—includes noPaper, doorOpen, jammed,offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull • A comma-separated list of error types. Valid error types include lowPaper, noPaper, lowToner, noToner, doorOpen, jammed, offline, serviceRequested, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputNearFull, outputFull, inputTrayEmpty, overduePreventMaint
ext-device.toshiba.show-printer-errors	When set to "Y", MFP errors will be shown on the Print Release page. Default: Y
ext-device.toshiba.no-access-on-printer-errors	When set to "Y", MFP errors will be shown on the Welcome page and the MFP will be locked down so that no operations are allowed. Default: N
ext-device.toshiba.no-access-on-printer-errors-text	OPTIONAL: Additional text displayed at the end of the welcome page when the MFP is in error. Default: None (no additional text is displayed)
ext-device.toshiba.v2.delete-suspended-jobs-on-logout	When set to "Y", any jobs in suspended state on the MFP (such as jobs which cannot continue because of an error on the MFP) will be deleted when the user logs out. Default: N
ext-device.toshiba.calculate-printer-errors-using-tray-data	When set to "Y", we will only consider the MFP to be in "No Paper" error state if all the trays of a particular paper size are out of paper. When set to "N", any tray out of paper will cause the MFP to be in error. Default: Y (always look at the MFP's tray data to determine "No Paper")
ext-device.toshiba.v2.force-account-mode	This configuration is only relevant to the case where a user's account selection mode is set so that they are not allowed to select their "personal account" and must choose a shared account.

	The possible values are: "DEFAULT", "quota" or "NONE". The "quota" mode will set the user's quota on login to zero on the MFP, so that they will not have any quota to do a copy or scan job. The quota will be updated for the shared account once the account is selected. When the mode is set to "NONE", then we do not force the user to select an account in any way. The "DEFAULT" mode is currently the same as "quota". Default: DEFAULT
ext-device.toshiba.show-job-status-button	Determines whether or not the Job Status button is displayed on the Print Release page. • 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. Default: “Y”

Note: The limit reference variables for version 2 quotas are used in a different way than the standard limit references such as *ext-device.toshiba.limit-reference.duplex*. The standard ones are used at log in time to decide if the user will have permission to do copies, assuming they are going to try to do at least one page of a certain page size and whether it will be duplex or not. The version 2 quota reference variables are used to set the page costs for quotas on the copier. For example, if PaperCut is told to charge $0.50 for A3 pages, and *ext-device.toshiba.v2.limit-reference.quota.large-paper-size* is set to A3, then this will tell the copier that large-pages cost $0.50.

5 Known Limitations and Security

5.1 Usability and User Interface Limitations

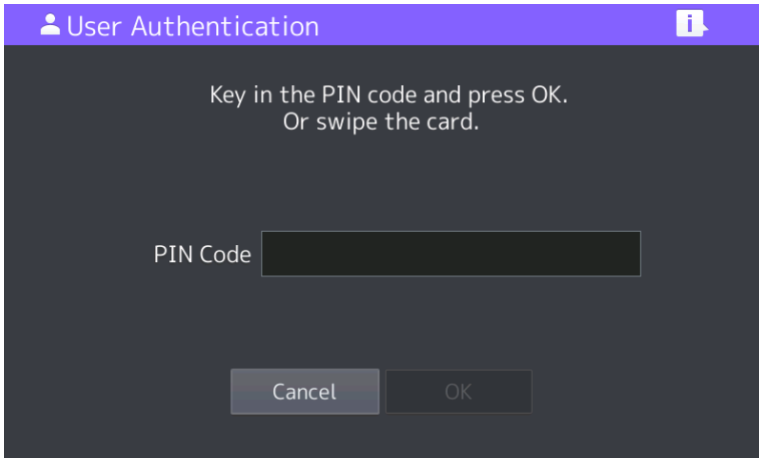
The Toshiba SDK provides no ability to customize the device login process and workflow. Instead PaperCut leverages the device’s built-in authentication by implementing a custom LDAP server. The Toshiba device connects to the PaperCut LDAP server to perform username/password, identity number and swipe card authentication.
The terminology used on the Toshiba screens sometimes differs to the terminology used by PaperCut. This may be confusing to users. Examples of this include:

- The user’s username is called “ID” on the Toshiba.
- A user’s PaperCut ID number is called a PIN on the Toshiba
- When using card + PIN authentication the PIN on the Toshiba **is** the PaperCut PIN.

When using ID number authentication, you may use the numeric keypad to enter the ID which will show up in the PIN field. In order to enter the username/password then you need

to click on the button, “ID/Password” (highlighted in red in the figure – note that the “ID” here is really referring to the “username”).

PIN Code screen on Toshiba e-BRIDGE Next series:



Toshiba PIN Input is used to enter the Identity Number for PaperCut

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.

The SDK2 integration allows PaperCut to lock the copier when the user has not selected an account. This is a significant improvement over earlier integration, however, this is not as preferable as being able to force account selection at login. Toshiba are aware of this issue and aim to improve their SDK for future devices.

5.2 Limited Authentication Options

Similar to section 5.1 above, the Toshiba SDK does not allow for customizing the authentication process. For this reason, PaperCut has the following limitations with login/authentication:

- No option for PIN entry when performing identity number authentication (the input for the identity number is actually done using Toshiba's PIN input).
- If card + PIN authentication is enabled and a user swipes an unknown card to perform card association, they will still be prompted for a PIN. The user must enter a PIN of "0" to allow them to login to the device to complete their card association. This is not ideal because there is no way to indicate to the user that their card is unknown and they must enter "0" as the PIN. This is a limitation of the Toshiba's LDAP-based card+PIN authentication.
  The user must enter "0" even if they already have a PIN number set (e.g. when using a previous card).PINs should be pre-assigned for the users, as the MFC will not prompt for new PINs if they are not defined.
- Identity number authentication was introduced in PaperCut MF version 13.
- Card authentication requiring PIN was introduced in PaperCut MF version 13.1.

5.3 Zero stop when Copying and Scanning

In SDK version 2, we have introduced the Zero Stop capability, enabling jobs to potentially be stopped part way through when the user runs out of quota in PaperCut. 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 their account. Toshiba's SDK version 2 offers the ability to limit page counts but has the following limitations:

1. The copier does not seem to stop immediately when limits are reached for copying. There is a small delay meaning that users can overrun their account below zero by about 2 pages. This can be avoided by using *ext-device.toshiba.v2.overrun-offset* and setting to an appropriate amount (please see the advanced configuration section for more details), however, there are drawbacks with doing this.
2. Ideally PaperCut would be informed of the user selection prior to copying or scanning and be able to accept/reject the job at this point. Current Toshiba API implementations prevent this level of pre-approval.
3. SDK version 2 supports the page costs of color, grayscale, small page size and large page size. It does not support costs or discounts for duplex and individual pages sizes other than the 2 sizes of small and large. By default, the small paper size is set to *ext-device.toshiba.v2.limit-reference.quota.small-paper-size* which is *US letter* in the United States and *A4* everywhere else. The large paper size is set to *ext-device.toshiba.v2.limit-reference.quota.large-paper-size* which is *Ledger* in the United States and *A3* everywhere else.

When the quota limit is exceeded a popup message on the device will alert the user to having run out of quota.

If the scanning is stopped midway through when scanning off the platen, then the Toshiba error message is different to above, instead it says, "*The quota has been reached. Only the previously scanned documents will be processed*". Scanning via the Automatic Document Feeder will not be interrupted midway through. If the scanning is denied from the outset, then the standard message above will be shown.

5.4 Zero stop when Faxing

Toshiba devices currently do not stop fax jobs mid-way when users run out of credit. Instead, users can complete the fax job and possibly incur an overdraft in their accounts.

5.5 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:

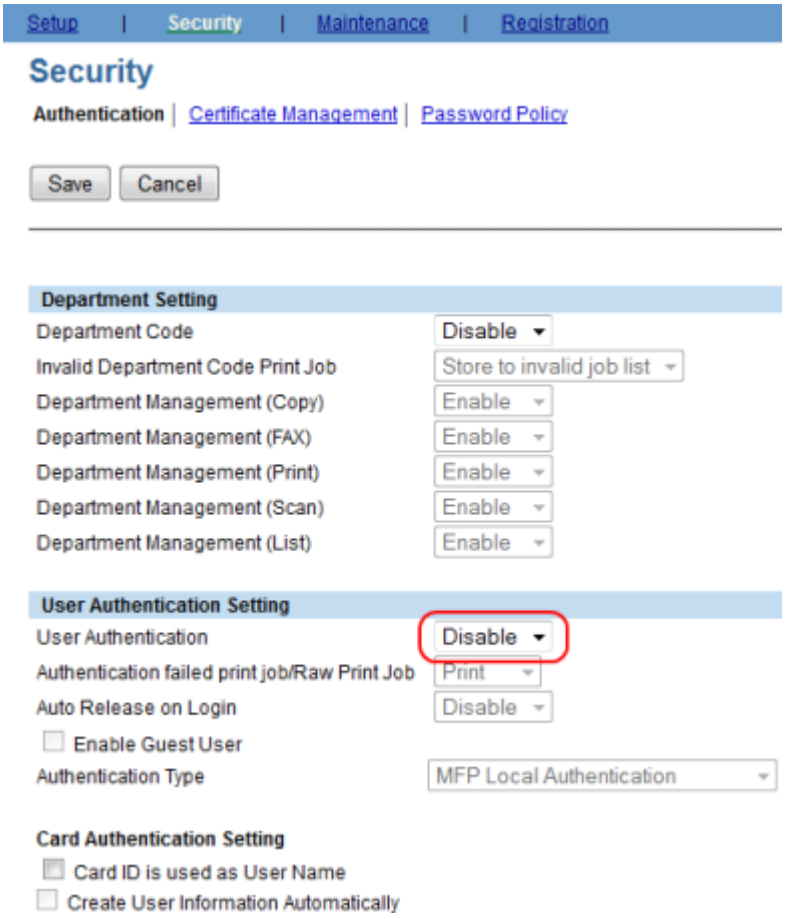
- The copier's built in admin password should be changed and always kept secure.
- The power and network cable should be securely connected. The system is designed to be robust and record copier usage if the power is lost during copying, but it is possible to start copying before the embedded application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

6 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.

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”.



6.1 Further optional uninstallation steps

Theoretically, you could reverse all the steps that you followed during the setup process. You could revert the 08 codes back to what they were and change all the TopAccess 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 ODCA option
- Disabling the Print Data Converter
- Unselecting the Job Quota Setting

7 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.
  - Check that the Device's administrator username and password are correct.
- Verify that the 08 service mode settings have been changed.
- Verify that ODCA has been enabled and the default port of 49629 was used.
- Verify the correct version of the firmware is running.

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

There are a number of possible reasons for this:

- A copy job tends to overrun its quota by at least 2 pages probably because there are at least 2 pages in the device which have not yet come out of the copier. This is a restriction of the device.
- You have used more advanced costs than just color, grayscale, small paper size or large paper size which are all that SDK2 provides direct support for. For example, you have set a duplex discount and by default we will favor the user and assume all pages are duplex (according to *ext-device.toshiba.v2.limit-reference.quota.duplex*).

You see the dialog about "Empty Quota" on the copier before you have actually run out of quota in PaperCut.

Check the following:

- Make sure that the Print Data Converter file is installed as mentioned in section 2.4.10. If this is not done, then print jobs (from a print server) by the user can potentially reduce the quota for that user on the copier.

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

Firstly ensure that you are using a compatible card reader (see Appendix A on page 47).

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. 3500)
- 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.

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 fails to address the issue then review the following:

1. Make sure that in the configuration of the LDAP server that the authentication type is set to *Simple Bind* as documented previously (section 2.4.8).
2. Make sure you are running PaperCut 13.0 or above and the latest device firmware.
3. On the device in TopAccess, switch off all DNS servers and enter all network addresses as IP numbers. Bad DNS server settings, or slow reverse DNS can slow down login times.

Card self-association is enabled but the user is still prompted for a PIN. If they enter their PIN it doesn't work. What is wrong?

If Card Authentication is requiring a PIN and card self-association is enabled, then the user must enter a PIN of "0" when prompted for a PIN. If they enter any other PIN including their own PIN associated with the PaperCut account, it will not work.

I have enabled Identity Number authentication in PaperCut but it doesn't prompt me for the ID number. Why not?

You may not have enabled PIN code authentication in TopAccess on the MFC. With the correct firmware on the MFC, you must enable "PIN Code Authentication" in the "PIN Code Authentication Setting" under the Security tab. This requires a firmware version that supports this feature. Please check your device firmware is at or above the version listed in section 2.3.1.

I have enabled Swipe Card requiring a PIN in PaperCut but it doesn't prompt me for the PIN. Why not?

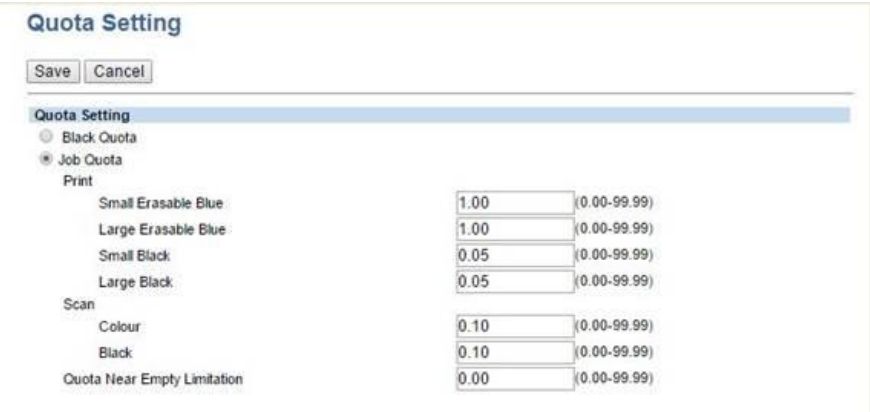
You may not have enabled "Require PIN Code" in the "Card Authentication Setting" in the Security tab in TopAccess. This requires the correct firmware on the MFC mentioned in section 2.3.1.

Users are unable to cancel their print jobs at the MFP. How can I fix this?

This is explained in section 2.4.10 for the Print Data Converter. Basically, to support the zero stop functionality, we have to force network print jobs to be owned by "printope" instead of the real username. Therefore, by default the MFP won't let the authenticated user delete the print jobs which it believes are owned by "printope". To override this, an 08 code needs to be set (it is also listed in the 08 code checklist in the appendix).

When a user chooses to copy using the Erasable Blue color option, why does the copy cost always default to 1.0 per page?

Even after setting copy color job costs for the "Small Erasable Blue" and "Large Erasable Blue" on the Admin web interface, the costs default to 1.00 on the device's web admin. To override this, manually set the copy color job costs on the device's web admin (**Counter > Quota Setting**) and click **Save**.



8 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 table below.

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 8.2)
e-Bridge IDGATE - HID iClass	3500	40002
e-Bridge IDGATE - Mifare	3500	30001
Generic Keyboard mode readers	3500	60001

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

8.1 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 **3500** setting to: **90001**.

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

8.2 Magtek Dynamag

Toshiba has 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.

8.3 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

8.4 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) and click **Update**

Standard Converters

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

`javascript:<path>`	Advanced: Define a custom conversion function in JavaScript (see below)

It is possible to chain or pipeline converters by delimiting with a pipe (|). For example, `ascii-enc|hex2dec` will first unpack the encoded ASCII number then convert it to a decimal.
Tip: Not sure which converter to use? Often trial and error is a good approach. After presenting a card, the number will appear in an application logger message with conversions applied (assuming the card is unknown to the system). Try different converters and inspect the resulting numbers in the application log.
Using custom JavaScript
If the inbuilt converter functions are unable to meet 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`

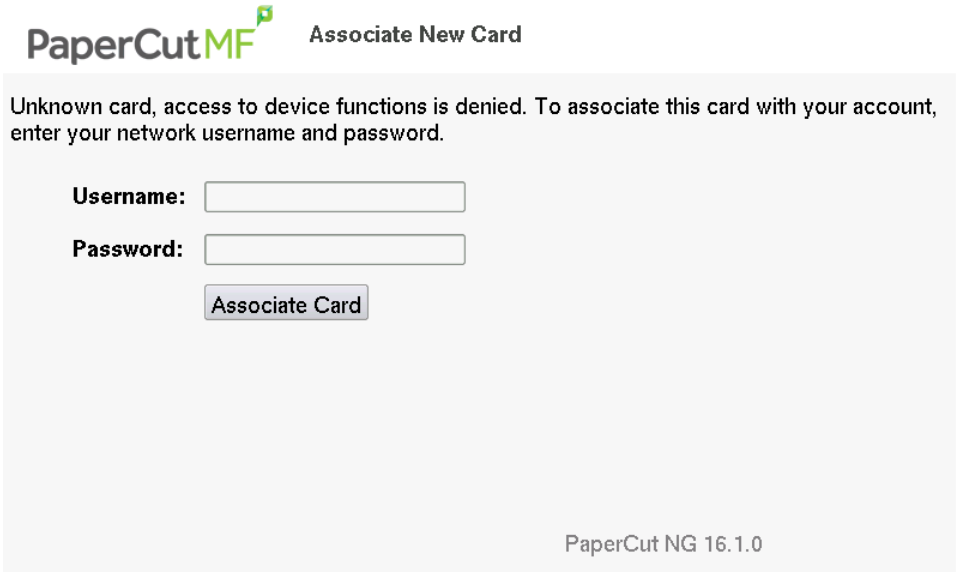
Tip: Check the file `[install-path]/server/log/server.log` when testing. Any scripting errors will be displayed as warning messages in the log.
Tip: A Javascript script may also be included in the pipeline. For example:
`ascii-enc|hex2dec|javascript:custom/card.js`
Other advanced notes

- 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.

9 Appendix B: 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.



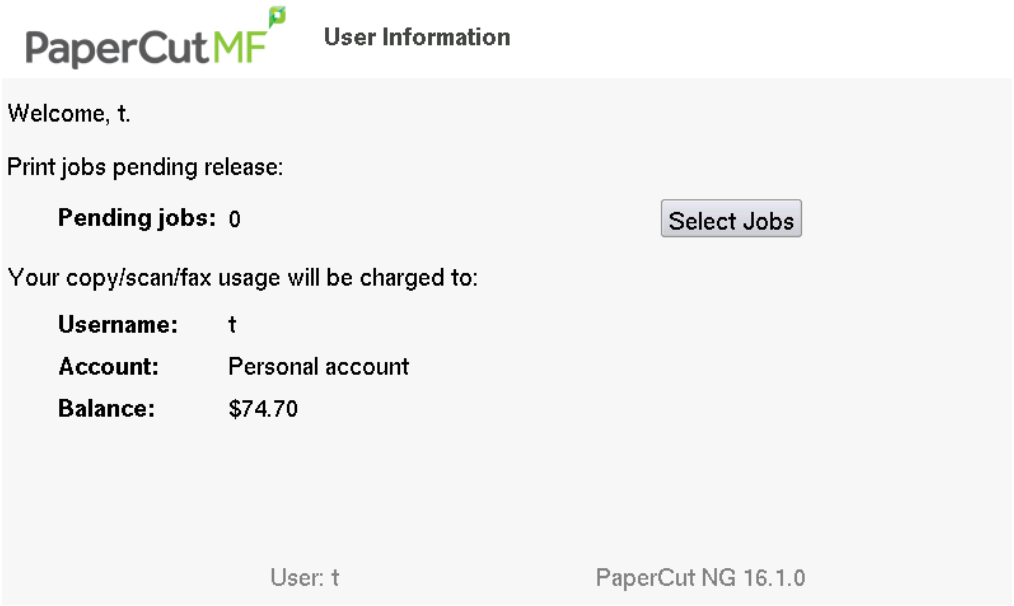
4. Enter the username and password. If the association is successful the user is notified on the LCD screen.
5. Logout (press the access key).

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.

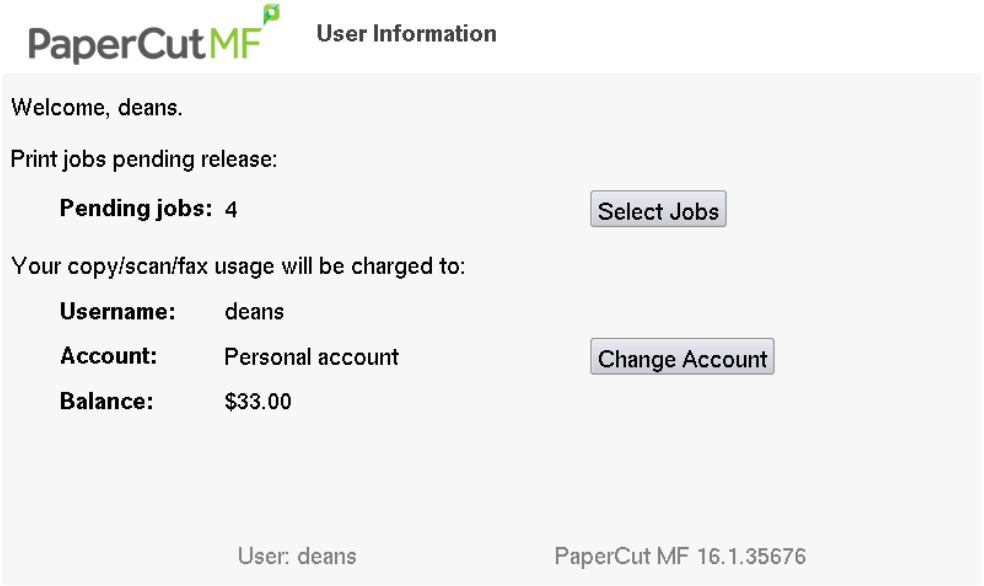
10 Appendix C: Device screenshots for user documentation

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

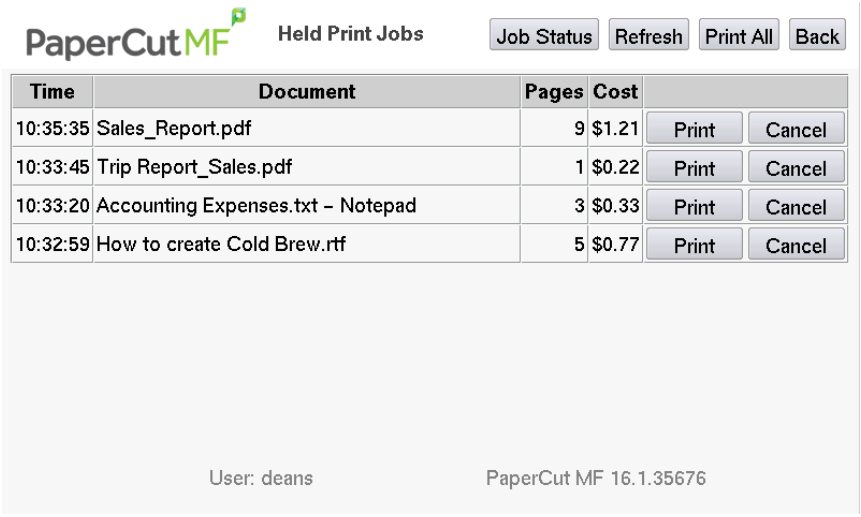
Welcome screen showing personal account and print release options:



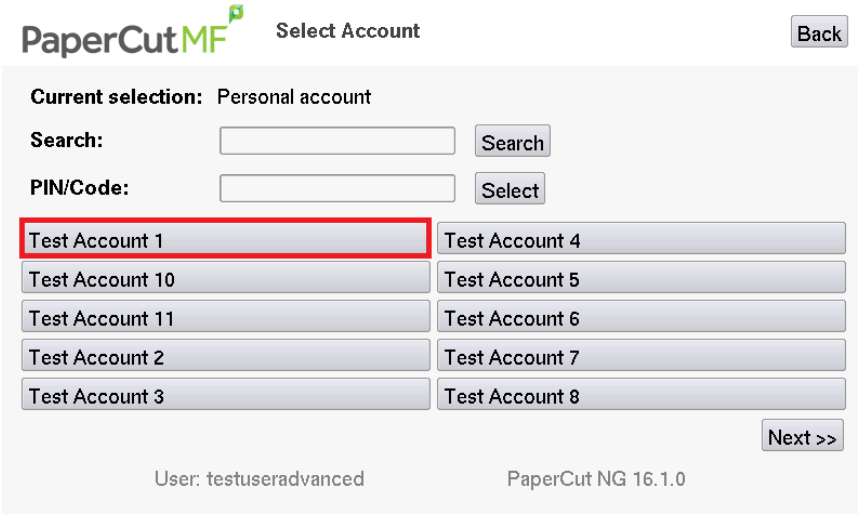
Welcome screen showing account selection options:



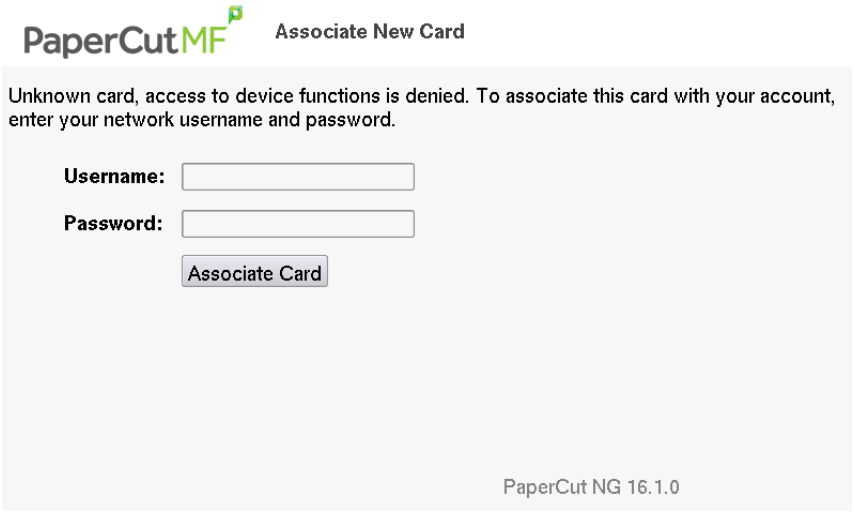
Print release screen showing the jobs awaiting release.



Shared account search / selection screen.



User card association



11 Appendix D: 08 Code Check list

Description	08 service code	service mode setting

Card Reader	3500	90001 (e.g. Elatec TWN3) – See Appendix A: Supported Authentication Card Readers
Card Authentication LDAP field	9398 (only in TopAccess with e-BRIDGE Next)	eBMUserCard
Zero Stop Enabling (in older firmware which does not display Quota Setting in TopAccess)	6086 (may not be available)	1
Extension Label (optional)	9955 (not required with e-BRDIGE Next)	PaperCut
Dedicated card swipe screen (optional)	8727	1 (to enable) or 0 (to disable)
Initial default screen be the EWB screen	9132	99
Change the “Menu” button to open the EWB directly (optional)	9985 (not required with e-BRIDGE Next)	1
Allow anyone to delete a print job	8726	1
Allow the user to delete their jobs from the Private/Hold screen on the copier	9236	3

12 Appendix E: TopAccess Settings Check list

Description	Menu
Configure EWB	Administration -> Setup -> EWB
Configure Server Registration Setting	Administration -> Setup -> EWB
Create LDAP server	Administration -> Maintenance -> Directory Service (menu location has changed for e-BRIDGE Next series)
Enable LDAP authentication in sections: 1. User Authentication	Administration -> Security

2. RBAC 3. PIN Authentication (in newer versions) 4. Card Authentication	
Import Print Data Converter (not required with e-BRIDGE Next)	Administration -> Setup -> Print Data Converter
ODCA Enabling	Administration -> Setup -> ODCA