

PaperCut Xerox Secure Access EIP 1.5+ Manual

Contents

1	Version history.....	4
2	Overview.....	5
2.1	Consistency.....	5
2.2	Integration.....	5
2.3	Rate of development.....	5
2.4	Vendor Neutral.....	6
2.5	Security.....	6
3	PaperCut embedded solution for Xerox EIP.....	7
4	Installation.....	9
4.1	Requirements.....	9
4.2	Migrating from EIP 1.0 to EIP 1.5+ Xerox Devices.....	9
4.3	Card Reader support.....	10
4.3.1	Network Card Readers.....	11
4.3.2	USB Card Readers.....	11
4.4	Setup Procedure.....	13
4.4.1	Introduction.....	13
4.4.2	Networking/Firewall Configuration.....	14
4.4.3	Enable the HTTPS/SSL protocol.....	14
4.4.4	SNMP version.....	15
4.4.5	Change the default Administrator password on VersaLink devices (EIP 3.7) .	18
4.4.6	Create/setup the Xerox device in PaperCut.....	20
4.4.7	Enable Xerox Secure Access (XSA) Authentication Settings.....	21
4.4.8	Verify Xerox Secure Access (XSA) Authentication Settings.....	26
4.4.9	Accounting Configuration on EIP 1.5 devices.....	29
4.4.10	Ensure copier functions only accessed by logging in.	30
4.4.11	Verify and Enable Extensible Interface Platform Settings.....	33
4.4.12	Verify Walkup Screen Preferences on VersaLink devices (EIP 3.7).....	34
4.4.13	Set up Integrated Scanning.....	34
4.4.14	(Optional) Enable network card reader.....	35

- 4.4.15 (Optional) Additional Network Security 35
- 5 Post-install testing 36
 - 5.1 Test preparation: create test users 36
 - 5.2 Simple printing and copying 37
 - 5.2.1 Test preparation: configure simple test user 37
 - 5.2.2 Simple printing 38
 - 5.2.3 Simple copying..... 40
 - 5.3 Advanced copying..... 42
- 6 Configuration 46
 - 6.1 Device Function 46
 - 6.2 Held print job settings at the device 47
 - 6.2.1 Held print jobs settings that can be changed at the device 47
 - 6.2.2 Held print jobs settings that can be viewed at the device 48
 - 6.3 Authentication Methods 48
 - 6.4 Configuring Swipe Card Readers 51
 - 6.5 Account selection 52
 - 6.5.1 By name and by code 52
 - 6.5.2 By name 53
 - 6.5.3 By code 54
 - 6.6 Single Sign On (SSO) 55
- 7 Advanced Configuration 55
 - 7.1 Config Editor 55
 - 7.2 Customizing the header logo and colors 69
 - 7.3 Setting an explicit PaperCut Server Network Address 69
- 8 Known Limitations and Security 70
 - 8.1 EIP 1.5 device limitations summary..... 70
 - 8.1.1 No Zero Stop for EIP 1.5 devices 70
 - 8.1.2 Less automatic configuration on EIP 1.5 devices 71
 - 8.1.3 Account selection and login without credit limitation for EIP 1.5 devices..... 71
 - 8.1.4 Login without credit *and* free scanning/faxing limitation on EIP 1.5 devices. 71
 - 8.1.5 Maximum of 30 concurrent fax jobs 73
 - 8.2 Faxing limitations summary..... 73
 - 8.2.1 Fax Tracking 73
 - 8.2.2 No Zero Stop for Faxing..... 73
 - 8.3 User Interface limitations summary 74
 - 8.4 Bypassing the System limitations summary 74



- 8.5 Card Reader support for authentication limitations summary 74
- 8.6 EIP 2.0+device limitations (Job Assembly not supported by default) 74
 - 8.6.1 Turning Off Job Limits' Preauthorization..... 74
- 8.7 Unable to bypass authentication for custom Apps/Services 77
- 8.8 Integrated Scanning limitations summary 78
- 9 How it works 79
- 10 FAQ & Troubleshooting 80



1 Version history

PaperCut MF version or date	Details
18.3.3	4.2 Migrating from EIP 1.0 to EIP 1.5+ Xerox Devices; 4.4.4 SNMP version; 4.4.6 Create/setup the Xerox device in PaperCut; 7.1 Config Editor; 10 FAQ & Troubleshooting
18.3.0	7.1 Config Editor
18.2.1	7.1 Config Editor
18.2.0	2 Overview; 5 Post-install testing; 6 Configuration; 7 Advanced Configuration
18.1.3	7.1 Config Editor
18.1.1	5 Post-install testing; 6.4 Shared Account Selection; 7.1 Config Editor

2 Overview

This manual covers the setup of Xerox Secure Access EIP 1.5+ (e.g. EIP 1.5, EIP 2.x, EIP 3.x, EIP 4.x). For general PaperCut MF documentation, please see the [PaperCut MF manual](#).

This manual provides an overview of the installation, configuration and operation of PaperCut's embedded software MFD (Multi-Function Device) solutions. Today's MFDs are smarter – they have touch screens and offer the ability to run applications directly on the device. The goal of the PaperCut Software's embedded MFD solution is to leverage these smart devices and to provide walk-up copier users with the same set of rich application features provided in the print control area. These include:

- Secure access to the device via user authentication
- Integration with single sign-on environments
- Print release of held print jobs (Secure & Find Me Printing)
- Monitoring, control and tracking of printing, copying, scanning, and faxing (Quotas, Charging, Allocation, Job Limiting, Zero Stop, and Logging)
- Integrated Scanning
- Card self-association and print release at login
- Allocation of printing, copying, scanning, and faxing costs to different accounts, departments, cost centers, or projects (Shared Accounts)
- Multiple ways to locate Shared Accounts
- Adding comments to invoices of Shared Accounts
- Customization of most device screens, including logos, colors, and messages
- Changing and viewing the settings of held print jobs at the device

Highlights of the embedded solution include:

2.1 Consistency

The embedded solutions are developed in-house by the PaperCut Software development team. This ensures that the copier interface is consistent with the workstation print interface, meaning users only have to learn one system.

2.2 Integration

PaperCut is a single integrated solution where print, internet and copier control are all managed in the one system. Users have a single account and administrators have the same level of reporting and administration for all services. The embedded solution interacts with the PaperCut server using a Service Oriented Architecture (SOA) and web services based protocols.

2.3 Rate of development

PaperCut is developed under a release-often policy where new features are made available to users as soon as they are complete. Unlike hardware based solutions, new versions can be delivered to users regularly as software updates.

2.4 Vendor Neutral

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

2.5 Security

A large percentage of PaperCut's user base operates in the Education environment where security is integral. All embedded solutions are developed with security in mind. Any security objectives that cannot be satisfied are fully disclosed.

3 PaperCut embedded solution for Xerox EIP

This document covers the latest PaperCut embedded solution, which supersedes the older Secure Access solution. It is recommended for all compatible Xerox devices running the firmware - Xerox Secure Access Extensible Interface Platform (EIP) version 1.5 or above. A list of compatible devices that support EIP can be found on the following website: <https://www.papercut.com/tour/embedded/xerox/>

The PaperCut embedded solution’s features differs based on the Xerox EIP firmware version:

PaperCut embedded solution features	EIP 1.5	EIP 3.0+
Accessing device functions securely (Xerox Secure Access), which allows the PaperCut server to authenticate users at the MFD	✓	✓
Setting-up and configuring devices more easily	✓	✓
Tracking and controlling copying, scanning, faxing, and USB printing	✓	✓
Integrated Scanning	✗	✓
Enforcing print quotas more strictly (Job Limits) Only for EIP 2.0+ devices	✓	✓
Preventing users from overrunning their available credit (Zero Stop enforcement of copy and scan jobs using Job Limits) Only for EIP 2.0+ devices	✓	✓
Multiple ways to locate Shared Accounts (full screen interface for Account Selection)	✓	✓
Commenting on accounts and other invoice options	✓	✓
Hiding the cost of a print job	✓	✓
Customizing logo and header colors	✗	✓
Supporting native keyboard	✗	✓
Home screen displaying all options - Print All, Print Release, and Integrated Scanning	✗	✓
Viewing and releasing individual print jobs (full screen interface for Print Release)	✓	✓
Releasing jobs from a hold / release queue	✓	✓
Multiple print jobs select when releasing print jobs	✗	✓

Releasing print jobs on login	✓	✓
Logging in with username, ID, and card	✓	✓
Setting a PIN on initial login	✓	✓

The PaperCut embedded solution’s UI differs based on the Xerox EIP firmware version:

PaperCut embedded solution UI

<i>Below EIP 3.0</i>	<i>EIP 3.0 and above</i>

4 Installation

This section covers the installation of the PaperCut embedded application for compatible Xerox devices running the firmware - Xerox Secure Access Extensible Interface Platform (EIP) version 1.5 or above.

4.1 Requirements

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

- PaperCut is installed and running on your network. Please see the 'Introduction -> Quick Start Guide' section of the PaperCut user manual for assistance.
- Your Xerox MFD supports the Extensible Interface Platform version 1.5 or higher.
- Your Xerox MFD has "Network Accounting" installed and enabled including off-box authentication support. (Network accounting is also known as JBA accounting.) You may need to contact Xerox to enable this functionality. **Please check with Xerox that the Network Accounting Kit license is still available because if the device has been declared as "End of Life", it may no longer be available.**
- You have available the network name and IP address of the system running PaperCut (e.g. the print server).
- The Xerox MFD is connected to the network.
- You have available the network address of the Xerox MFD. It is recommended that the MFD is configured with a static IP.

4.2 Migrating from EIP 1.0 to EIP 1.5+ Xerox Devices

If you have an existing Xerox device that supports EIP 1.5+ and exists in PaperCut as an EIP 1.0 device, then you may want to convert this device into an EIP 1.5+ device in PaperCut. Currently, there is no support for doing this directly in the PaperCut admin interface. You could take screenshots of the device's details tabs of: Summary, Advanced Charging and Filters and Restrictions. Then delete the old EIP 1.0 device and create the new EIP 1.5+ device filling in the details based on your previous screenshots.

Please note that what was previously in PaperCut called an EIP 2.0+ device in the database is equivalent to what we now call an EIP 1.5+ device (they are both stored in the same way in the database unlike the EIP 1 device). Therefore, there is no need to convert from an EIP 2.0+ device to EIP 1.5+ because any previously defined EIP 2.0+ devices will now show up in PaperCut as EIP 1.5+ devices.

An alternative more advanced method to do the conversion using a command line tool is to change the device type in the PaperCut database. To do the conversion from EIP 1.0 to EIP 1.5+, you will need to do the following steps (where in this example the printer name to change is called "*device/XeroxPrinter*" as you would see for the Device Name in the Device List):

1. Stop the PaperCut Application Server
2. Start a command prompt
3. On Mac/Linux, `sudo su – papercut`
4. `cd [app-path]/server/bin/<platform>/`
5. `db-tools run-sql "update tbl_printer set device_type = 'EXT_XEROX_EIP2' where device_type = 'EXT_XEROX_CAA' and display_name = 'device\XeroxPrinter'"`
6. Start the PaperCut Application Server.
7. Log in to the PaperCut MF Admin web interface.
8. Navigate to **Devices**.
9. Select the EIP 1.5+ device that is migrated from EIP 1.0.
10. On the **Devices > Device Details > Summary** page's **External Device Settings**, update the following fields:
 - **Device's administrator username** – Ensure this is the same as the device web interface's administrator username.
 - **Device's administrator password** – Ensure this is the same as the device web interface's administrator password.
 - **SNMP v3 privacy password (Optional)** –
 - If you want PaperCut MF to use SNMP v2c and it is enabled in the device's web interface, then ensure this is blank.
 - If you want PaperCut MF to use SNMP v3 and it is enabled in the device's web interface, then ensure this is the same as the device web interface's **Privacy Password / Encryption Password**.

Note: For more information, see [4.4.4 SNMP version](#).
 - **SNMP v3 authentication password (Optional)** –
 - If you want PaperCut MF to use SNMP v2c and it is enabled in the device's web interface, then ensure this is blank.
 - If you want PaperCut MF to use SNMP v3 and it is enabled in the device's web interface, then ensure this is the same as the device web interface's **Authentication Password**.

Note: For more information, see [4.4.4 SNMP version](#).

4.3 Card Reader support

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

Xerox devices can support 2 general classes of card readers:

- Network card readers (i.e. not physically connected to the MFP. The PaperCut server communicates with these over the network)
- USB card readers directly connected to the Xerox device (some recent Xerox devices with updated firmware now support a limited number of USB card readers – contact Xerox for details).

The Network Card Reader option will work with any Xerox device supporting “Xerox Secure Access”.

4.3.1 Network Card Readers

Network card readers may be used on any Xerox device. PaperCut supports two cost effective network card readers:

- Elatec TWN3 with the TCP Converter
- RFideas Ethernet card readers

These readers are available directly from the card reader distributors and PaperCut Authorized Solution Centers in your region.

These network card readers are located on the MFP device and are connected to the network. When a user swipes their card at the reader the card number is sent to the PaperCut server for validation. If the card number is valid the user will be granted access to the MFP.

4.3.2 USB Card Readers

Xerox updated their platform in late 2011 to support USB card readers through Xerox Secure Access. Devices supporting USB card readers include:

- ColorQube 8700/8900 (firmware 071.160.222.26601 and above)
- ColorQube 9301/9302/9303 (firmware 061.180.222.32100 and above)
- WorkCentre 5890
- WorkCentre 72xx
- WorkCentre 75xx (firmware 061.121.222.21500 and above)
- WorkCentre 78xx
- VersaLink devices (EIP 3.7)

The following card readers are supported by Xerox:

- Proximity card readers – RFideas, Elatec TWN3, Elatec TWN4 (on some models)
- Magstripe card readers – Magtek, “IDTech MiniMag”, RF Ideas MS3-00M1AKU
- Barcode card readers - Honeywell (3800G04), Motorola (DS9208, DS457) – from PaperCut 15.2

PaperCut should generally support the USB card reader if the particular Xerox Model and firmware version support it. Up to date information on this compatibility can be obtained from Xerox. The PaperCut software only interprets the XML data about the card reader that is sent to it from the MFP (via Secure Access API) – if the card reader is not sending this information then PaperCut can do nothing about reading the data and there must be an issue or incompatibility between the Xerox MFP and the card reader.

4.3.2.1 USB Card Reader Plug-in

VersaLink devices require a USB Card Reader Plug-in to use the supported USB Card Readers in combination with Xerox Convenience Authentication.

To install the USB Card Reader Plug-in:

1. Go to the Xerox site: http://www.support.xerox.com/support/versalink-b405/file-download/enin.html?operatingSystem=win7x64&fileLanguage=en_GB&contentId=136885&from=downloads&viewArchived=false
2. Download the zip file: Cardreader_plugin_with_signature.zip
3. Extract the cardreader_sig.jar file from the downloaded zip file to a convenient location on your computer.
4. Log into the device's web admin.
5. Select **System > Plug-in Settings**.

Plug-in Settings

Authentication on Registration

Plug-in Feature

Close

6. Slide **Plug-in Feature** to the right so it is in the checked position.

Plug-in Settings

Platform Version 2.0.0

Authentication on Registration

Plug-in Feature

Plug-ins

Plug-in Name	Status
1 CAC & PIV Smartcard Service Plugin	Deactivated
2 CCID Terminal Plugin	Deactivated
3 ActiveTagPlugin	Activated

Close

7. When prompted, select **Restart Now**.
8. When the system is back online, select **System > Plug-in Settings**.
9. Log into the device's web admin.
10. Select **System**.
11. Select **Plug-in Settings**.
12. Select **Add**.

Plug-in Settings

Platform Version 2.0.0

Authentication on Registration

Plug-in Feature

Plug-ins Add

Activate Deactivate Details Open

Plug-in Name	Status
1 CAC & PIV Smartcard Service Plugin	Deactivated
2 CCID Terminal Plugin	Deactivated
3 ActiveTagPlugin	Activated

Close

13. Browse to the location of the cardreader_sig.jar file you previously extracted from the .zip file.
14. Select **OK**.
15. Select **Close**.
16. Reboot the printer to activate the plug-in.
17. When the system is back online, select **System > Plug-in Settings**.
18. Log into the device's web admin.
19. Select **System**.
20. Select **Plug-in Settings**.
21. Ensure the status for the plug-in Xerox USB Car Reader (CR 3.0.04 or later) is "Activated".

Plug-in Settings

Platform Version 2.0.0

Authentication on Registration

Plug-in Feature

Plug-ins Add

Activate Deactivate Details Open

Plug-in Name	Status
1 CAC & PIV Smartcard Service Plugin	Deactivated
2 CCID Terminal Plugin	Deactivated
3 ActiveTagPlugin	Activated
4 Xerox USB Card Reader (CR.3.0.04)	Activated

Close

22. Select **Close**.
The plug-in is now ready for use.

4.4 Setup Procedure

4.4.1 Introduction

This procedure describes the process of setting up Xerox Secure Access EIP 1.5+ using the Xerox ColorQube 8700 (EIP 2) as an example. This part of the setup is similar between the

EIP 1.5 and 2.0 devices. The specific steps, screen layouts and button/label names can differ between device models. However the general process is the same for all supported devices.

4.4.2 Networking/Firewall Configuration

Ensure that your networking/firewall configuration allows:

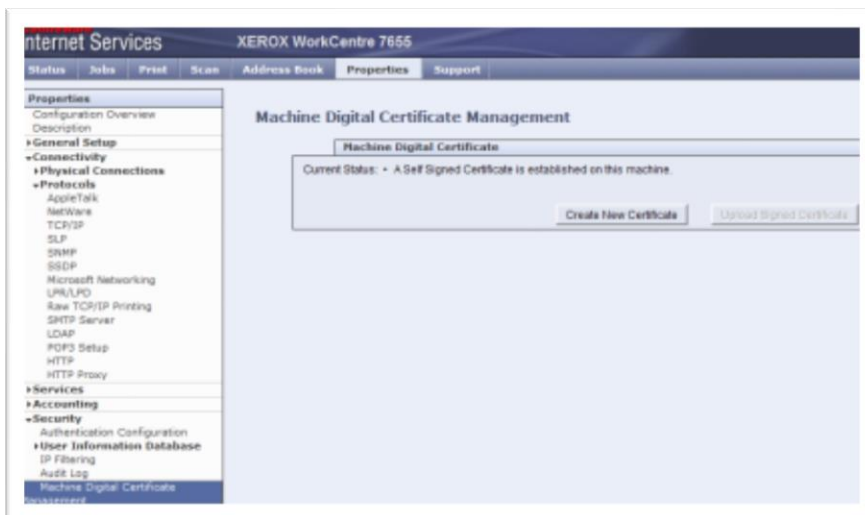
- inbound connections from the Xerox devices to the PaperCut server on ports 9191 and 9192.
- outbound connections from the PaperCut server to the Xerox device on ports 80 and 443.

4.4.3 Enable the HTTPS/SSL protocol

Xerox Secure Access requires the use of HTTPS/SSL for communications. This must be enabled before completing any of the subsequent steps.

This involves generating an SSL certificate for the device:

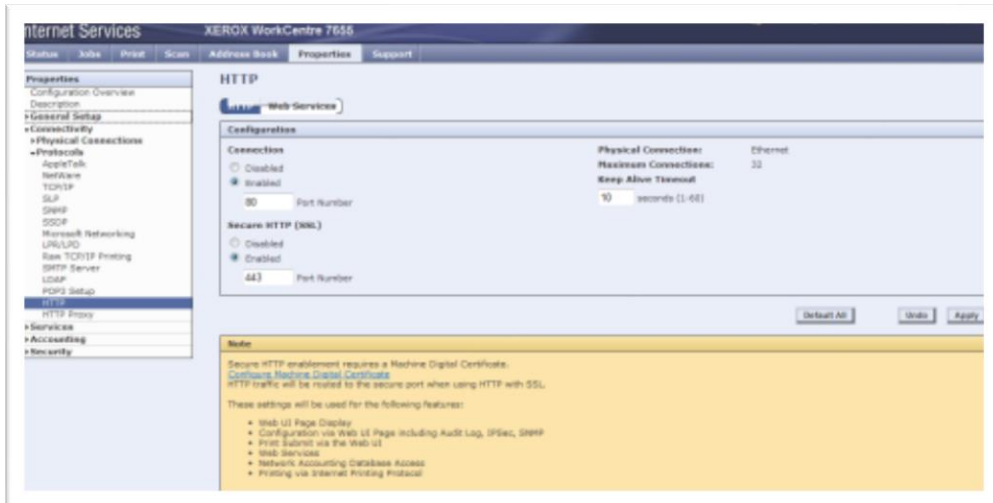
1. Login to the device's web admin.
2. Navigate to Properties->Security->Machine Digital Certificate Management
3. Press "Create New Self Signed Certificate".



4. Complete the required information
5. Press Apply.

Now enable the HTTP/SSL/TLS protocol:

1. Navigate to Properties->Connectivity->Protocols->HTTP
2. Enable the "Secure HTTP (SSL)" option



3. Press Apply

4.4.4 SNMP version

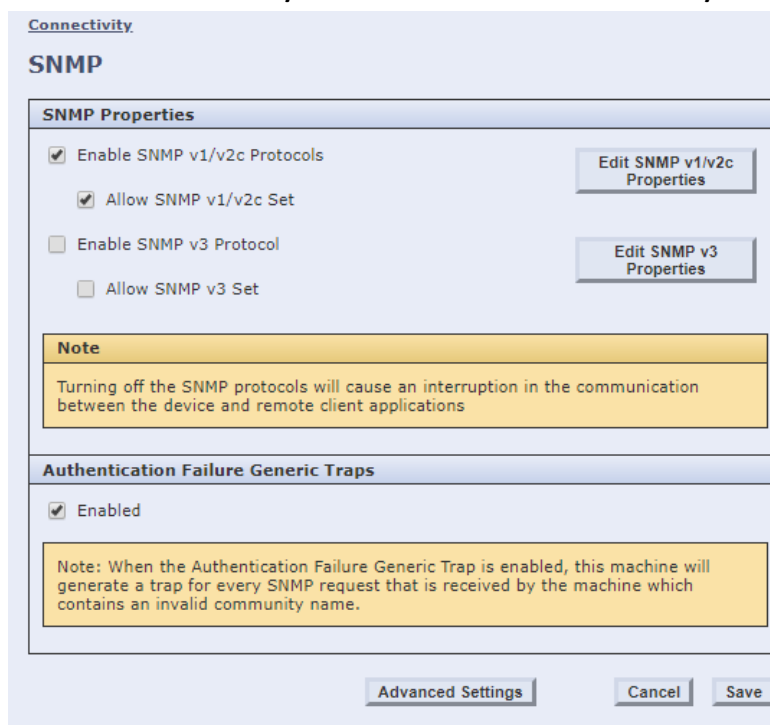
You can configure PaperCut MF to use any one of the following:

- SNMP v2c, or
- SNMP v3

4.4.4.1 SNMP v2c

If you want PaperCut MF to use SNMP v2c, then:

1. On the device’s web interface, ensure to enable SNMP v2c:
 - i. Login to the device’s web interface.
 - ii. Navigate to **Properties > Connectivity > Setup > Protocol > SNMP**.
 - iii. Select **Enable SNMP v1/v2c Protocols** and **Allow SNMP v1/v2c Set**:



- iv. Click **Edit SNMP v1/v2c Properties**.
- v. In **GET Community Name**, **SET Community Name** and **Confirm SET Community Name**, enter relevant values.

Take note of the **SET Community Name**.

- vi. Click **Save**.
2. On the PaperCut MF Admin web interface, while installing PaperCut MF, ensure **SNMP v3 privacy password** and **SNMP v3 authentication password** are blank:

3. On the PaperCut MF Admin web interface, after installing PaperCut MF, ensure the value of the config key **ext-device.xerox.snmpv2.set-community-name** is the same as the device web interface's **SET Community Name**.

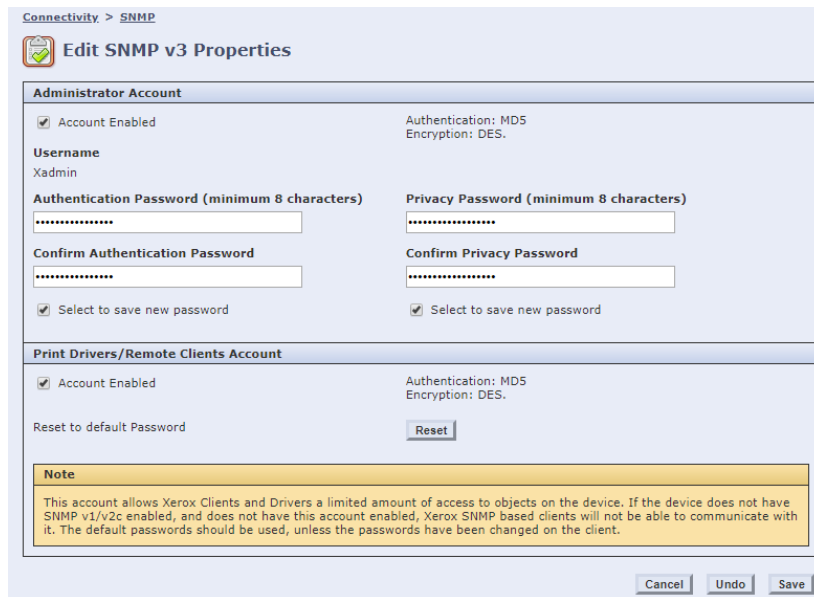
4.4.4.2 SNMP v3

If you want PaperCut MF to use SNMP v3, then:

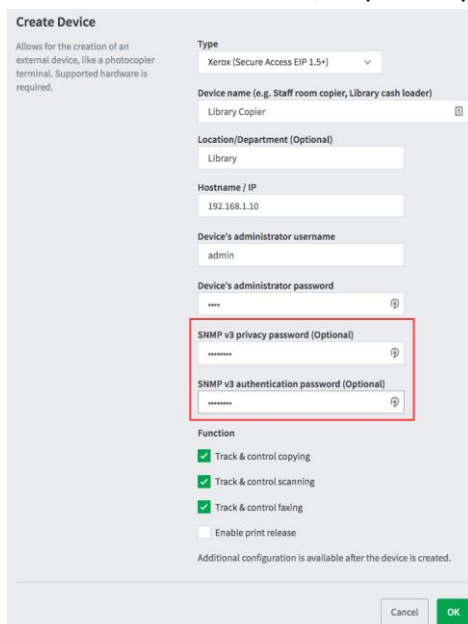
1. On the device's web admin interface, ensure to enable SNMP v3:
 - i. Login to the device's web admin interface.
 - ii. Navigate to **Properties > Connectivity > Setup > Protocol > SNMP**.
 - iii. Select **Enable SNMP v3 Protocol** and **Allow SNMP v3 Set**:

- iv. Click **Edit SNMP v3 Properties**.
- v. In **Administrator Account**, select **Account Enabled**.
- vi. Take note of the **SNMP v3 Authentication Username/ Security Name**:

- vii. In **Authentication Password** and **Privacy Password / Encryption Password**, enter relevant values and take note of them.



2. On the PaperCut MF Admin web interface, while installing PaperCut MF, ensure **SNMP v3 privacy password** and **SNMP v3 authentication password** is the same as the device web interface's **Privacy Password / Encryption Password** and **Authentication Password**, respectively.

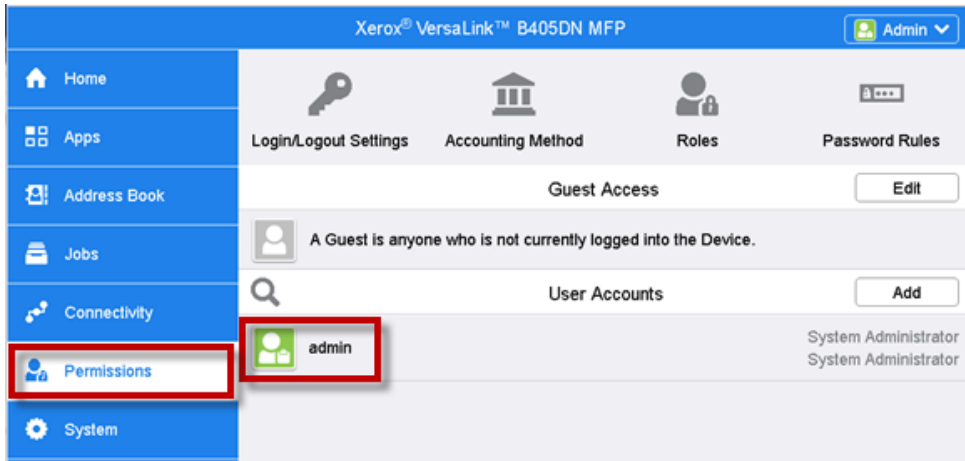


4.4.5 Change the default Administrator password on VersaLink devices (EIP 3.7)

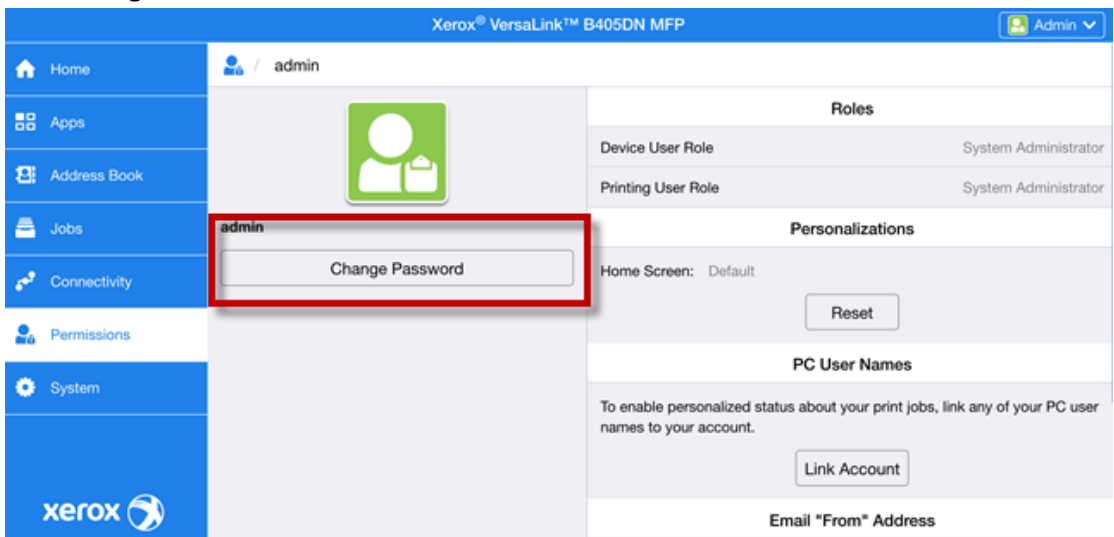
The default Administrator password must be changed on VersaLink devices (EIP 3.7). This is a pre-requisite to allow Xerox Secure Access (XSA) to be enabled on VersaLink devices (EIP 3.7). For more information on enabling XSA, see Section 4.4.7 Enable Xerox Secure Access (XSA) Authentication Settings.

To change the default Administrator password:

1. Login to the device's web admin (CWIS).
2. Navigate to Permissions > admin



3. Click **Change Password**.



4. Enter the relevant details

Change Password

Old Password

New Password

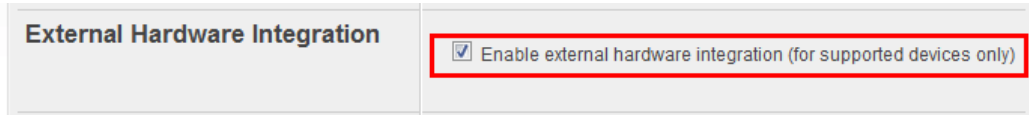
Retype New Password

5. Click **OK** to apply the changes.

6. Restart the device.

4.4.6 Create/setup the Xerox device in PaperCut

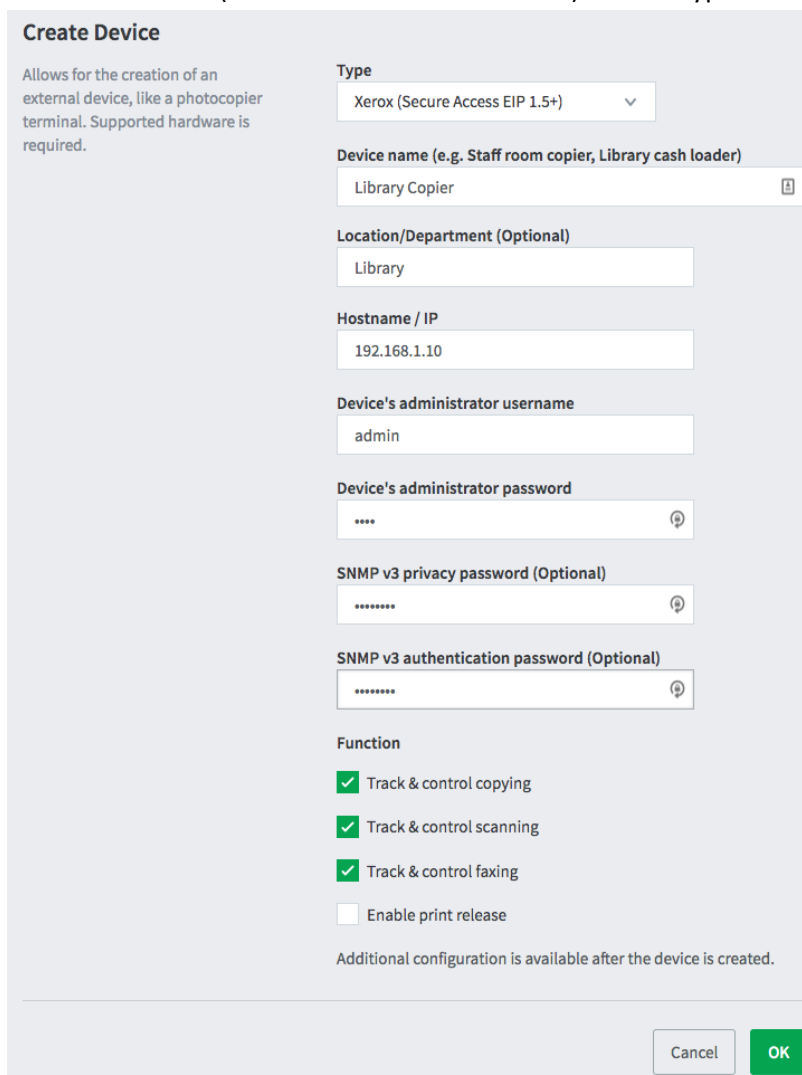
1. Log in to the PaperCut administration interface using a web browser (e.g. <http://papercut-server:9191/admin>).
2. Navigate to 'Options -> Advanced' and ensure the option 'Enable external hardware integration' is enabled.



External Hardware Integration

Enable external hardware integration (for supported devices only)

3. Press 'Apply'.
4. Navigate to the 'Devices' tab.
5. Click "Create Device" action from the left.
6. Select the "Xerox (Xerox Secure Access EIP 1.5+)" device type.



Create Device

Allows for the creation of an external device, like a photocopier terminal. Supported hardware is required.

Type: Xerox (Secure Access EIP 1.5+)

Device name (e.g. Staff room copier, Library cash loader): Library Copier

Location/Department (Optional): Library

Hostname / IP: 192.168.1.10

Device's administrator username: admin

Device's administrator password: ****

SNMP v3 privacy password (Optional): *****

SNMP v3 authentication password (Optional): *****

Function:

- Track & control copying
- Track & control scanning
- Track & control faxing
- Enable print release

Additional configuration is available after the device is created.

Cancel OK

7. Enter your own choice of a descriptive name for the device under "Device name".
8. Enter the Xerox device's IP address under "Hostname/IP".
9. Optionally enter your own choice of location/department information.
10. Enter the device administrator username and password (e.g. "admin" and "1111").

Note: This must be the same as the Administrator details used to log in to the device's web admin (CWIS).

11. Depending on which protocol (SNMP v2c or SNMP v3) you want PaperCut MF to use and which one is enabled on device's web interface, configure the following fields accordingly:

- For SNMP v2c - ensure **SNMP v3 privacy password** and **SNMP v3 authentication password** are blank.
- For SNMP v3 - ensure **SNMP v3 privacy password** and **SNMP v3 authentication password** is the same as the device web interface's **Privacy Password / Encryption Password** and **Authentication Password**, respectively.

For more information, see [4.4.4 SNMP version](#).

12. Under "Function" tick the options you would like to enable. E.g. "Track & control copying".

13. Click "OK".

PaperCut will try to connect to the device to configure various options over SNMP and SOAP/HTTPS.

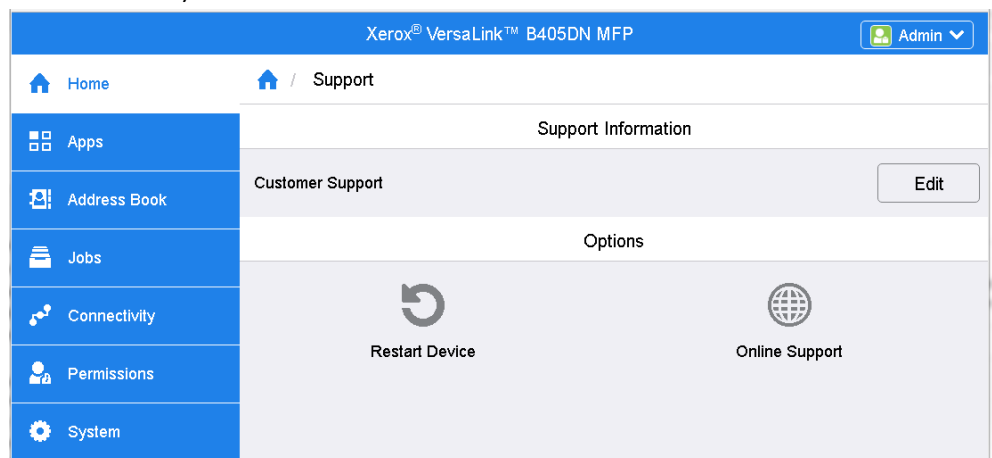
After the device is configured, the device status is displayed.

14. Verify that there are no device status errors.

Note: If the device status displays "Error: Xerox HTTP error calling:

`https://192.168.2.101/acct/get_config - Response: 404 (Not found)`", it can be due to a failure to configure the Xerox Network Accounting on the device.

- If you have a VersaLink device, restart your device (Home -> Support -> Restart Device).



- If you have other devices, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.

4.4.7 Enable Xerox Secure Access (XSA) Authentication Settings

At this point the Xerox Secure Access can be enabled. While on some devices, XSA gets enabled automatically via SNMP, others require XSA to be manually configured and enabled via the device's web admin page. Some devices (like the VersaLink devices, EIP 3.7) require the default Administrator password to be changed, as a pre-requisite before enabling XSA. For more information, see [4.4.5 Change the default Administrator password on VersaLink devices \(EIP 3.7\)](#).

4.4.7.1 Enable XSA on ColorQube 8700 (EIP 2)

On some devices such as the 8700, XSA can be enabled this way:

1. Log into the device's web admin.
2. Navigate to Properties->Login Methods->Web Service Enablement.
3. Click Edit.

Authentication & Accounting		
Enable	Name	Status
<input checked="" type="checkbox"/>	Xerox Secure Access	Enabled
<input checked="" type="checkbox"/>	Authentication & Accounting Configuration	Enabled
<input checked="" type="checkbox"/>	Session Data	Enabled
<input checked="" type="checkbox"/>	Job Limits	Enabled

4. Enable the tick box for Xerox Secure Access.

4.4.7.2 Enable XSA settings on WorkCentre 5325 (EIP 1.5)

On some devices such as the 5325, XSA can be enabled this way:

1. Log into the device's web admin.
2. Navigate to Properties->Security->Authentication Configuration.

Authentication Configuration > Step 1 of 2

Authentication Configuration

Login Type:

Print Stored File from Folder: Enabled

Folder to PC / Server: Enabled

Non-account Print: Enabled

Guest User:

Guest Passcode:

Retype Guest Passcode:

Use Domain Name for Print Client Authentication:

3. Ensure that the "Login Type" is set to "Xerox Secure Access"
4. Navigate to Properties->Security->Remote Authentication Servers->Xerox Secure Access Settings
5. Enable "Local Login" and "Get Accounting Code".

Note: "Local Login" and "Get Accounting Code", must be enabled manually even when XSA is enabled automatically via SNMP.

Xerox Secure Access Settings

Xerox Secure Access Server

Default Prompt:

Default Title:

Local Login: Enabled

Get Accounting Code: Enabled

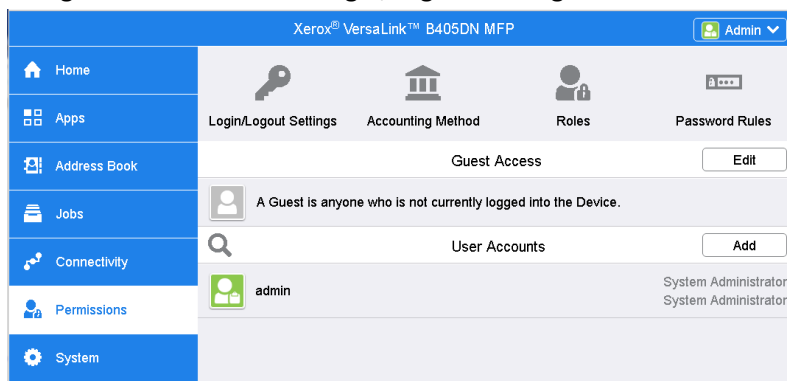
Connection Time-Out: Seconds(1 - 300)

4.4.7.3 Enable XSA settings on VersaLink devices (EIP 3.7)

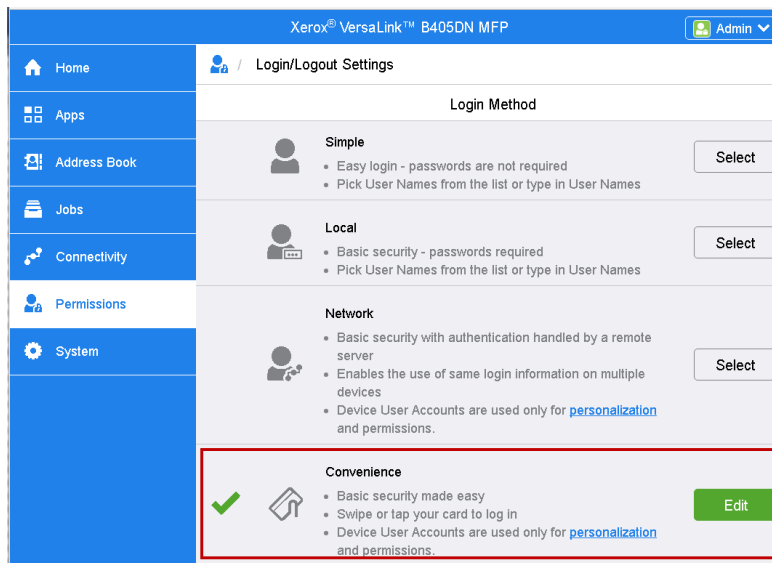
Note: Before attempting to enable XSA on VersaLink devices (EIP 3.7), ensure that the default Administrator password has been changed. For more information, see [4.4.5 Change the default Administrator password on VersaLink devices \(EIP 3.7\)](#).

XSA can be enabled this way:

1. Log into the device's web admin.
2. Navigate to Permissions->Login/Logout Settings.



3. In the "Convenience" Login Method, click "Edit".



4. In "Alternate Login", set the "Allow users to log in without their card?" to "Yes", if users can log in using other methods apart from just their identity cards.

Convenience Login

Server

IP Address : Port* 10.100.66.157 : 9192

Path device/xerox-conv-auth/sc

Alternate Login

Allow users to log in without their card?

Yes

No

Accounting Codes

Get codes automatically from server.

Users must manually enter codes at the Device.

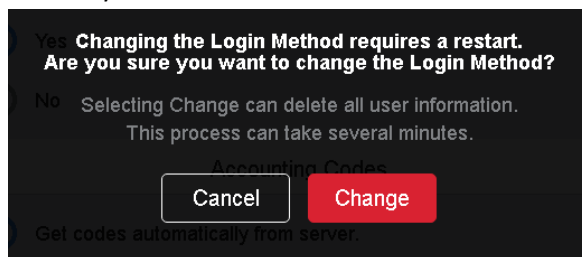
Device Website Login Method

✓ Local

Network

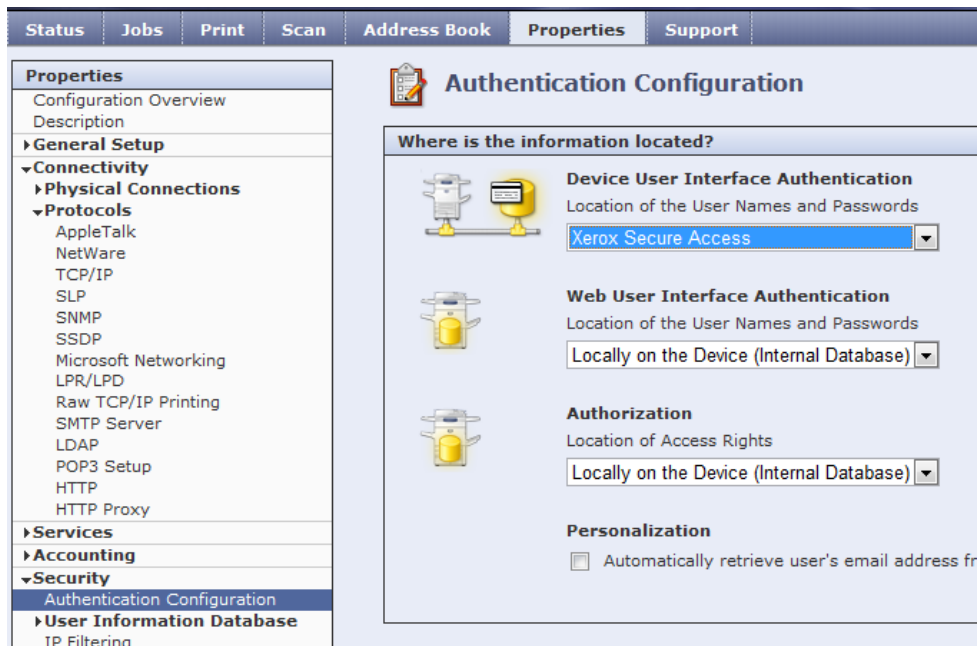
* Required

5. Click “OK” to apply the changes.
6. Restart your device.

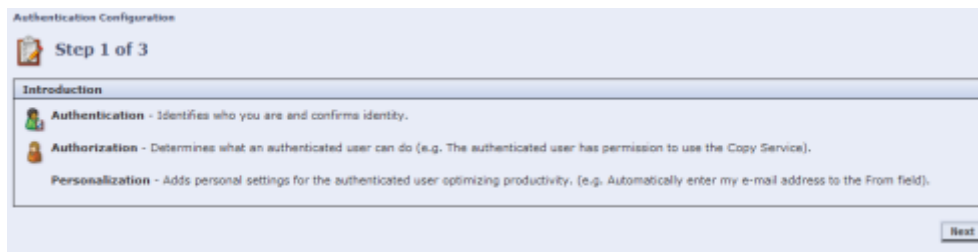


4.4.7.4 Enable XSA on some other devices

1. Log into the device’s web admin.
2. Navigate to Properties->Security->Authentication Configuration.



3. Select Next.



4. Change Device User Interface Authentication to Xerox Secure Access and press Next
5. Click on Configure for Device User Interface Authentication



4.4.8 Verify Xerox Secure Access (XSA) Authentication Settings

Once XSA is enabled ensure that the settings are correct.

4.4.8.1 Verify XSA on ColorQube 8700 (EIP 2)

1. Navigate to Properties->Login Methods->Xerox Secure Access Setup.

Authentication Configuration

Xerox Secure Access Setup

Remote Server Configuration Summary

IP Address:
10.100.66.100:9192

Device Log In Method
Xerox Secure Access Device + Alternate on-screen method

Apply Accounting Codes
Yes

Embedded
No

Version:

Device Instructional Blocking Window

Window Title (Reference 1)

Instructional Text (Reference 2)
Swipe your authentication card or press the 'Keyboard / Alternate Login' button to login and gain access to the device.

Instructional Blocking Window

Manual Override

This option allows you to override the remote server settings for this device.

[Manually Override Settings](#)

2. Click on Manually Override Settings

Authentication Configuration

Xerox Secure Access Setup

Remote Server Configuration Summary

IP Address: 10.253.100.67:9192

Device Log In Method: 0

Apply Accounting Codes: Yes

Embedded: No

Device Instructional Blocking Window

Window Title (Reference 1):

Instructional Text (Reference 2): Press the 'Keyboard / Alternate Login' button to login and gain access to the device.

Instructional Blocking Window

Manual Override

This option allows you to override the remote server settings for this device.

[Manually Override Settings](#)

3. Verify that the correct PaperCut Server IP Address is listed
4. Verify that the Login Methods is set to Xerox Secure Access + alternate on-screen authentication.
5. Verify that it will automatically apply Accounting Codes from the server

Xerox Secure Access Setup

Manual Override

Server Communication

IPv4 Address IP Address: Port
 Host Name

192 . 168 . 2 . 45 : 9192

Path
 device/xerox-conv-auth/soap/?deviceId=30030

Embedded
 Enabled
 Version:

Device Log In Methods

Xerox Secure Access Device Only (e.g., Swipe Cards)
 Xerox Secure Access Device + alternate on-screen authentication method


Accounting Information (Requires Network Accounting)

Automatically apply Accounting Codes from the server
 User must manually enter accounting codes at the device

Device Instructional Blocking Window

Window Title (Reference 1)

Instructional Text (Reference 2)
 Press the 'Keyboard / Alternate Login' button to login and gain access to the device.



Instructional Blocking Window

4.4.8.2 Verify XSA on WorkCentre 5325 (EIP 1.5)

This is difficult to do as there is not a corresponding "Properties" sub-menu in the admin interface with all the settings of the Xerox Secure Access. However, a print out of the Configuration Report does show the Xerox Secure Access Settings. This can be initiated from the panel of the device. The relevant subsection is near the end of the report. Verify the following settings:

- Server name/address is the same as the PaperCut Application Server name/address
- The port number is 9192.
- The service path is of the format: "device/xerox-conv-auth/soap?deviceId=xxxx" where xxxx is some number
- Local Login is enabled.
- Get Accounting Code is enabled.

The report looks like:

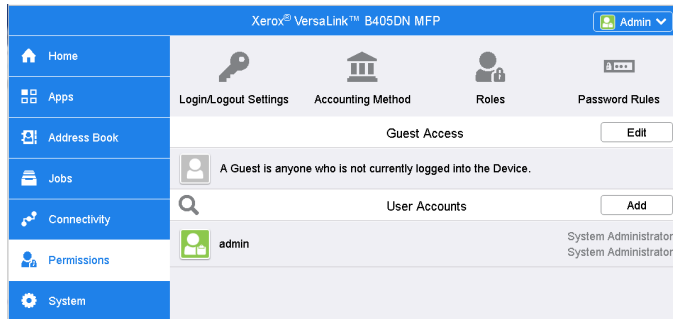
Xerox Secure Access

Server Name / IP Address	"10.100.66.75"
Port Number	9192
Service Path	"device/xerox-conv-auth/soap?deviceId=5005"
Local Login	Enabled
Get Accounting Code	Enabled

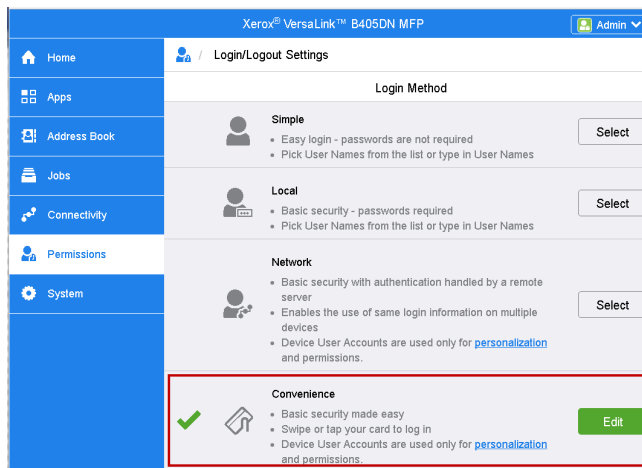
4.4.8.3 Verify XSA on VersaLink devices (EIP 3.7)

To verify if XSA is enabled on VersaLink devices:

1. Log into the device's web admin.
2. Navigate to Permissions->Login/Logout Settings.



3. In the "Convenience" Login Method, click "Edit".



4. Verify the following settings are configured:
 - "IP Address" is the address of the PaperCut Application Server
 - "Port" is "9192"
 - "Path" is "device/xerox-conv-auth/soap/?deviceId=xxxx" where xxxx is an auto-generated device id.
 - "Accounting Codes" is "Get codes automatically from server."

Convenience Login

Server

IP Address : Port* 10.100.66.157 : 9192

Path device/xerox-conv-auth/sc

Alternate Login

Allow users to log in without their card?

Yes

No

Accounting Codes

Get codes automatically from server.

Users must manually enter codes at the Device.

Device Website Login Method

✓ Local Edit

Network Select

* Required

Cancel OK

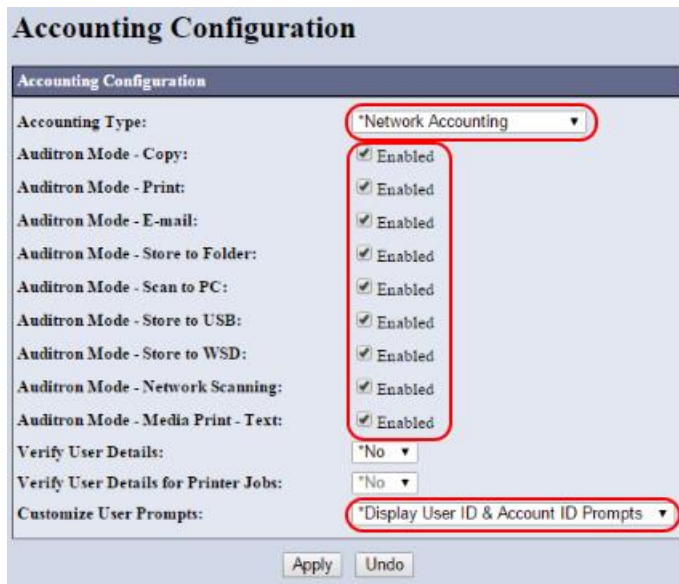
4.4.9 Accounting Configuration on EIP 1.5 devices

For EIP 2.0 or later devices, the accounting configuration is performed for you by PaperCut, whereas for EIP 1.5 devices, manual configuration in the device CWIS is required. Follow the instructions in this section if you are installing an EIP 1.5 device.

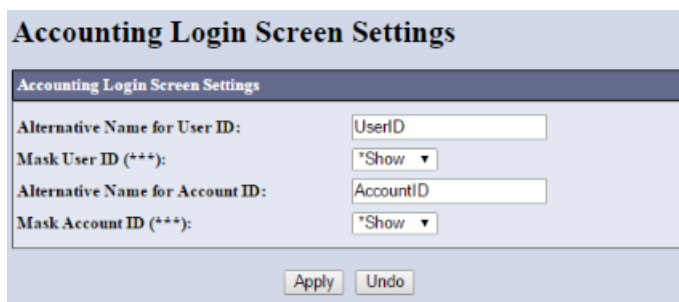
One of the main Accounting settings required is to turn on the User and Accounting prompts. The Prompts are used to ensure the user is tracked correctly in the Print Job Log and also that the account is tracked correctly for EIP 1.5 (in EIP 2.0+, the account is tracked by another method). Note that this setting is not used by PaperCut to prompt the user for authentication despite its name.

4.4.9.1 Set the User and Account Prompts on WorkCentre 5325 (EIP 1.5)

1. Log into the device's web admin.
2. Navigate to Properties->Accounting->Accounting Configuration.
3. Ensure the "Accounting Type" is set to "Network Accounting".
4. Ensure all the Auditron Modes are enabled.
5. Ensure that the User Prompts are set to: "Display User ID & Account ID Prompts".



6. Navigate to Properties->Accounting->Accounting Login Screen Settings.
7. Ensure the Alternative Name for the User ID is set to "UserID"
8. Ensure the Alternative Name for the Account ID is set to "AccountID"

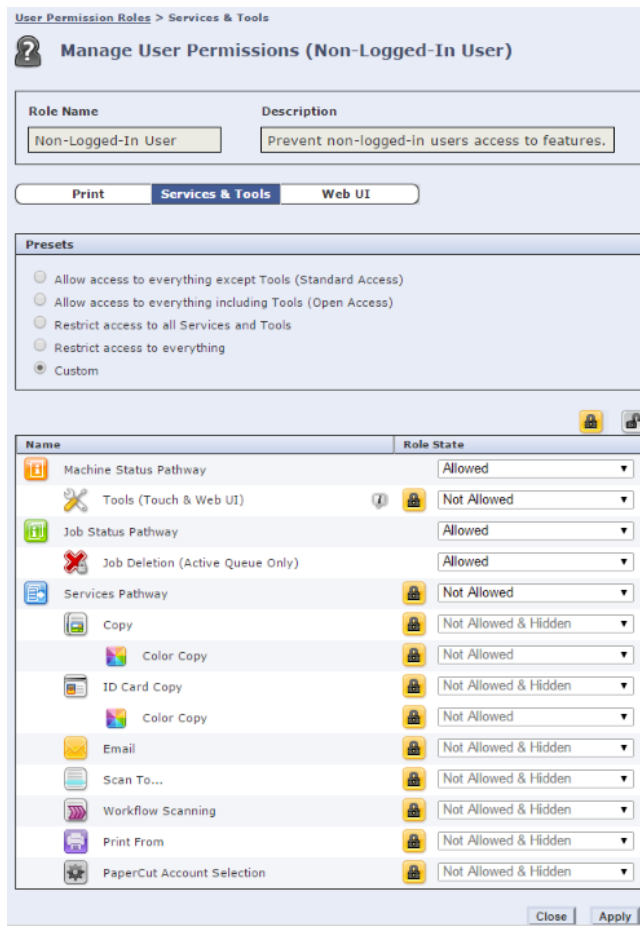


4.4.10 Ensure copier functions only accessed by logging in.

It is important to make sure that a user cannot access copier functions other than through the XSA authentication methods.

4.4.10.1 Access Control on ColorQube 8700 (EIP 2)

1. On some new devices, the Services Pathway can be found by navigating to: Properties -> Login/Permissions/Accounting -> User Permissions -> User Permission Roles -> Non-logged in Users -> Edit -> Services and Tools.



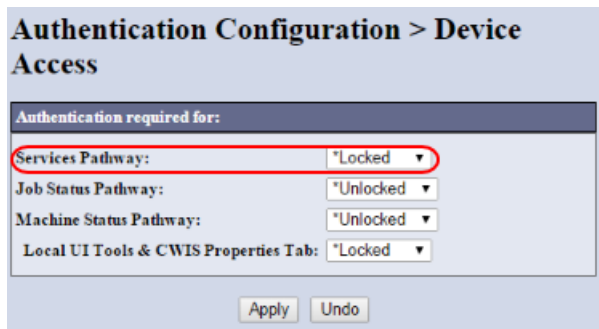
2. Ensure that non-logged in users cannot access the relevant services by setting to "Not Allowed".

4.4.10.2 Access Control on WorkCentre 5325 (EIP 1.5)

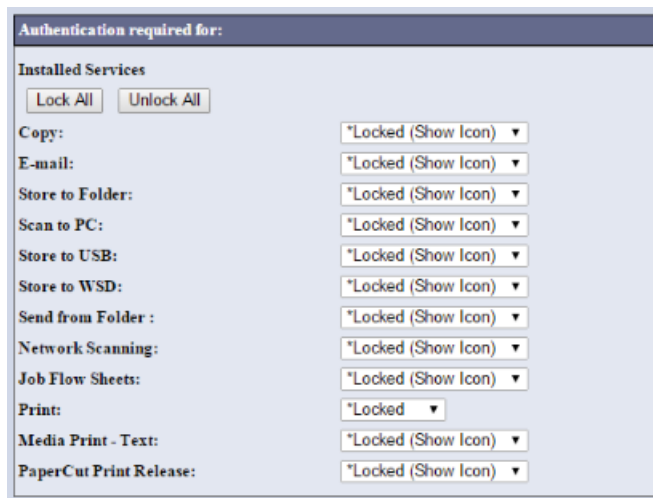
1. Navigate to Properties->Security->Authentication Configuration.
2. Click on Next to go to "Step 2 of 2".
3. Navigate to the Device Access page.



4. Change the Services Pathway setting to Locked. This locks access to the copier functions unless the user is logged in.



5. Navigate to Properties->Security->Authentication Configuration.
6. Click on Next to go to "Step 2 of 2".
7. Navigate to the Services Access page.



Ensure all the services are locked including the "PaperCut Print Release" service. Click apply when you are finished. You may be prompted to reboot for the settings to take effect.

4.4.10.3 Access Control on Other Devices

On other devices, it is done differently:

1. Navigate to Properties->Security->Authentication Configuration.
2. Navigate to the device access page.
3. Change the Services Pathway setting to Locked. This locks access to the copier functions unless the user is logged in



NOTE: On newer devices the Pathway Options screen may look different such as the

screen below



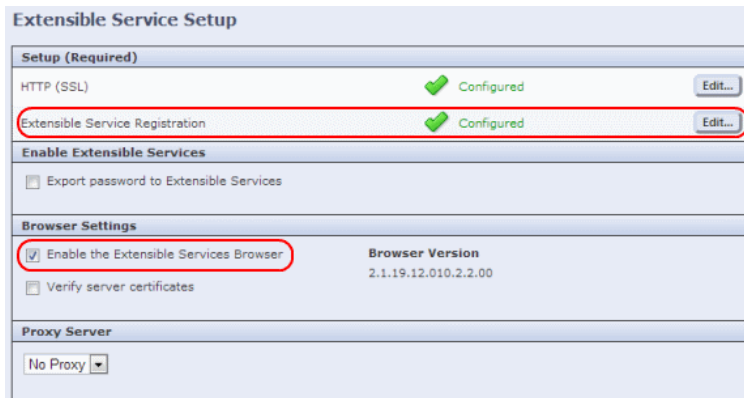
You may need to reboot the device for the settings to take effect.

Once the device is rebooted the device should display a screen to log in. Perform testing and verify you can log in and that copies are tracked by PaperCut.

4.4.11 Verify and Enable Extensible Interface Platform Settings

On some platforms such as the Xerox WorkCentre 75xx series and WorkCentre 5325, the EIP settings may not be enabled by default. Please verify the settings and enable if necessary.

1. Log into the device's web admin.
2. Navigate to Properties->General Setup->Extensible Service Setup



3. Verify that the Extensible Service Browser is enabled.
4. Click on the Extensible Service Registration Edit... button.

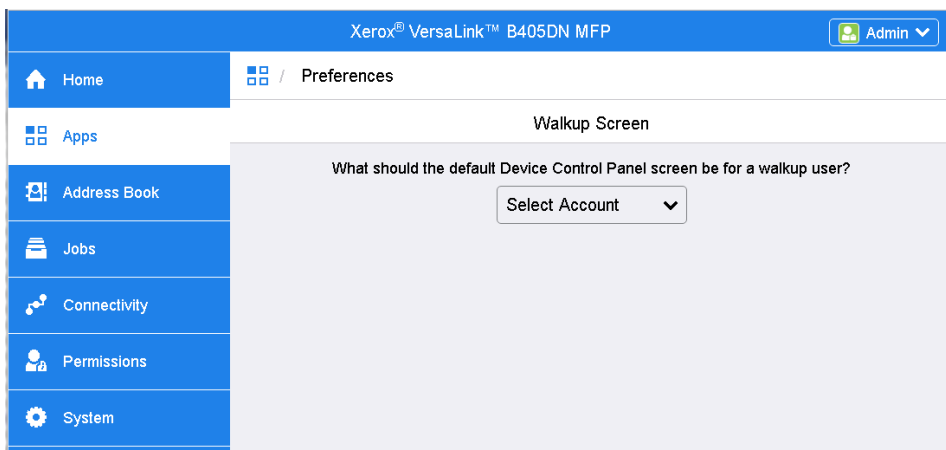


5. Verify that the Extensible Service Registration and User Interface Configuration items are enabled.

4.4.12 Verify Walkup Screen Preferences on VersaLink devices (EIP 3.7)

To verify Walkup Screen Preferences on VersaLink devices (EIP 3.7):

1. Log into the device's web admin.
2. Navigate to Apps->Preferences.
3. Verify that the default Device Control Panel screen for a walkup user is set to "Select Account" or "Print Release".



4.4.13 Set up Integrated Scanning

The PaperCut embedded application includes Integrated Scanning, which you can optionally enable per device. Integrated Scanning has the following additional device prerequisites:

- The firmware of the device must be EIP 3.0 or higher and must also be the latest version of that firmware, released by Xerox.
- To prevent cancelled scan jobs from triggering a device report print job, in the Services > Workflow Scanning > General Settings, set the **Confirmation Sheet** setting to **Off**.

4.4.14 (Optional) Enable network card reader

This section describes how to configure a network card reader for authentication at the MFP. For more information on the supported card readers see Section 4.3 Card Reader support.

To enable the network card reader:

1. Log into the PaperCut administration interface using a web browser (e.g. <http://papercut-server:9191/admin>).
2. On the “Devices” tab, select the MFP device.
3. Under the “Authentication Methods” option, enable the “Swipe Card” authentication option.
4. Select the “Enable network card reader” option.
5. Enter the network address and the port of the network card reader.



The screenshot shows the 'Authentication methods' configuration page. A red box highlights the 'Swipe card' section, which includes the 'Enable network card reader' checkbox, the 'Hostname / IP' text box containing '192.168.1.123', and the 'Port' text box containing '7778'. Other options like 'Username and password', 'Identity number', 'Require PIN', and 'Enable self-association with existing user accounts' are also visible but not highlighted.

6. Press “OK” or “Apply” to save the changes.
7. At this point PaperCut will establish the connection to the card reader. The status of the connection to the network card reader is displayed below the settings. If there is a problem connecting to the card reader any errors will be displayed here.

4.4.15 (Optional) Additional Network Security

The MFP communicates with the PaperCut server over the network (e.g. to authenticate users or release print jobs). To provide an additional level of security, PaperCut may be configured to only allow device connections from a restricted range of network addresses. This ensures that only approved devices are connected to the PaperCut server.

By default PaperCut will allow device connections from any network address. To restrict this to a subset of IP addresses or subnets:

1. Log into the PaperCut administration web interface at <http://<papercut-server>:9191/admin>
2. Go to the Options→Advanced tab and find the “Security” section.
3. In the “Allowed device IP addresses” field enter a comma-separated list of device IP addresses or subnets (in the format <ip-address>/<subnet-mask>).
4. Press the “Apply” button.
5. Test the devices to ensure they can continue to contact the PaperCut server.

5 Post-install testing

After PaperCut MF is installed on the device (i.e. device registration and integration is completed), it is recommended that you test some common usage scenarios. This is important for two reasons:

- To ensure that PaperCut MF works as expected.
- To familiarize yourself with the features and functionality of PaperCut MF.

This section covers the following post-install testing scenarios for *PaperCut MF – Xerox (Secure Access EIP 1.5+)*:

- [5.2 Simple printing and copying](#)
- [5.3 Advanced copying](#)

5.1 Test preparation: create test users

To execute the post-install testing scenarios, ensure at least two test users are created:

- **Simple test user** – A user who performs simple printing and copying.
- **Advanced test user** – A user who performs advanced copying.

To create test users:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options**.
3. In Internal **User Options**, select **Enable internal users**.
4. Click **Apply**.

Internal User Options

Provides management of user accounts in addition to those in the configured source.

[More Information...](#)

Enable internal users

Access control

Only admins can create users

Prefix usernames with: (optional)

guest-

Confirmation message

Thank you for registering. Your details are:
Full Name: %full_name%
Username: %username%
Password: %password%
Identity Number: %sid_num%

Also email confirmation message to user

Apply

5. Navigate to **Users**.
6. Click **Create internal user...**

- Enter the relevant details for the test users as required (simple test user, advanced test user):

The screenshot shows the 'Create Internal User' form in the PaperCut MF Admin interface. The form is titled 'New User Settings' and includes the following fields:

- Username:** Simple Test User
- Full Name:** Simple Test User
- Email Address:** simpletestuser@papercut.com
- Password:** ****
- Verify Password:** ****
- Identity Number:** [Empty field]
- ID PIN:** [Empty field]
- Verify ID PIN:** [Empty field]
- Email confirmation message to user:**

At the bottom right, there are 'Cancel' and 'Register' buttons. The 'Register' button is highlighted in green.

- Click **Register**.

5.2 Simple printing and copying

5.2.1 Test preparation: configure simple test user

To test the simple test scenarios, ensure at least one simple test user is created. For more information, see [5.1 Test preparation: create test users](#). Once created, ensure the simple test user is configured.

To configure the simple test user:

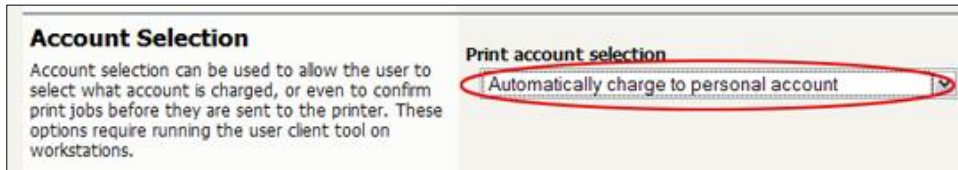
- Log in to the PaperCut MF Admin web interface.
- Navigate to **Users**.
- From the **User List**, select the simple test user.
- In the **Account Details** area, set the **Balance** to **\$50.00** and select **Restricted**:

The screenshot shows the 'Account Details' form for a user. The form includes the following fields:

- Balance:** \$50.00 (adjust)
- Restricted:**
- Overdraft:** Use default overdraft (\$0.00)

The 'Balance' field and the 'Restricted' checkbox are circled in red in the image.

- In the **Account Selection** area's **Print account selection**, select **Automatically charge to personal account**:



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

Print account selection
Automatically charge to personal account

- Click **Apply**.

5.2.2 Simple printing

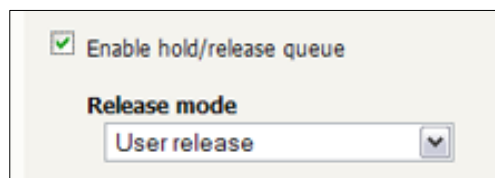
Simple printing does not involve providing the simple test user with a choice of accounts to choose from. Printing is charged to the simple test user's default My Personal Account.

To test simple printing, ensure the following test preparation requirements are met:

- Simple test user** - A simple test user is created and configured. For more information, see [5.1 Test preparation: create test users](#) and [5.2.1 Test preparation: configure simple test user](#).
- Printer queue settings** - The printer queue's Hold/Release Queue Settings are configured. For more information, see the [PaperCut MF manual](#).

To configure the printer queue's Hold/Release Queue Settings:

- Log in to the PaperCut MF Admin web interface.
- Navigate to **Printers**.
- Select the Printer that is applicable to the device being tested.
- In the **Hold/Release Queue Settings** area, select the **Enable hold/release queue**.



Enable hold/release queue

Release mode
User release

- Click **Apply**.
Print jobs to this printer queue are held until released by a user.

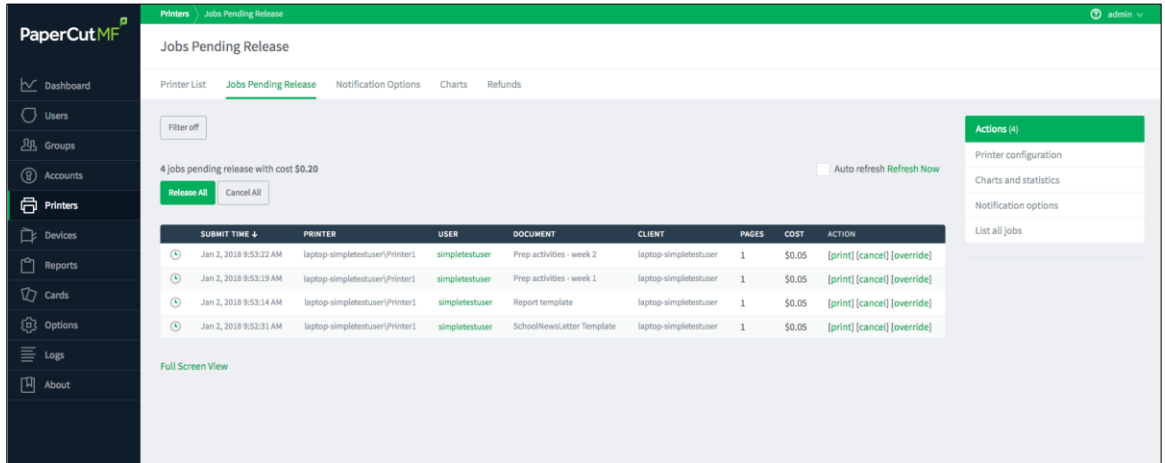
- Device functions** – The printing function is enabled.

To enable the printing function:

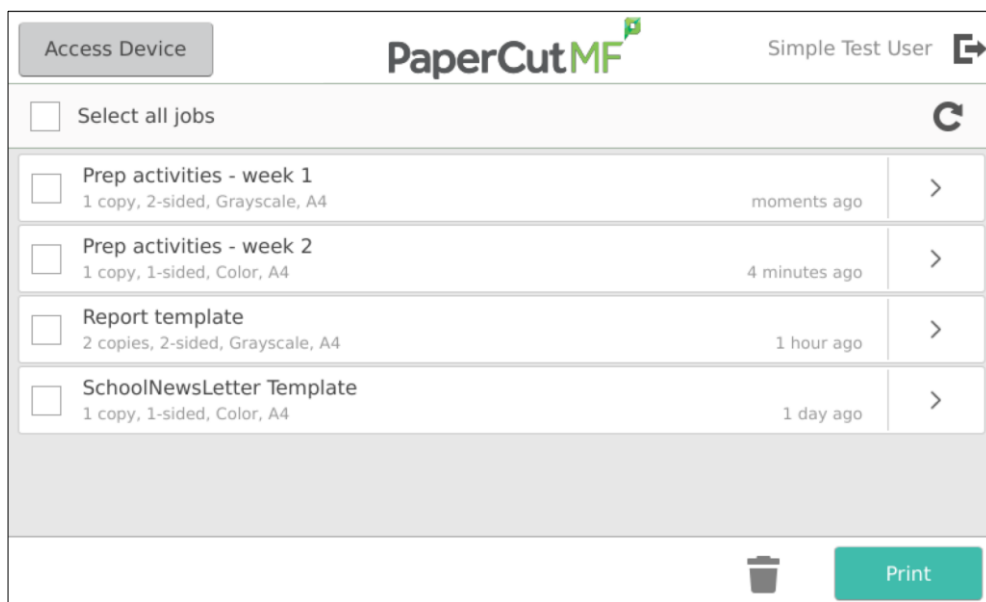
- Log in to the PaperCut MF Admin web interface.
- Navigate to **Devices**.
- Select the device being tested.
- In the **Print Release** area, select **Enable print release**.
- In the **This device will display jobs for release from the selected source queues**, select at least one source queue for print release that corresponds to this device's configured printer queue.
- Click **Apply**.
- Verify that the **Devices > External Device List** displays the device with **Print Release** in the **Function** column.

To test simple printing:

1. Log in to a computer as the simple test user.
2. Print a few jobs to the source queue that was selected in the **Devices > External Device List > Device Details > Print Release > Enable print release** area of the device being tested.
3. Log in to the PaperCut MF Admin web interface.
4. Navigate to **Printers > Jobs Pending Release**.
5. Verify that the print jobs for the simple test user are being held and listed:



6. Log out of the PaperCut MF Admin web interface.
7. Log in to the device as the simple test user.
8. Verify that the print jobs for the simple test user are being held and listed:



Note: You may be able to change the settings of held print jobs on the PaperCut MF Print Release screen before releasing them. For more information, see [6.2 Held print job settings at the device](#).

9. To release one or many held print jobs at once, select all the relevant held print jobs and click **Print**.
10. To delete one or many held print jobs at once, select all the relevant held print jobs and click the **Bin** icon.
11. To view and take actions on a single held print job, click the chevron:



Details of the held print job are displayed:

Field	Value	Field	Value
Time	Jun 22, 2018 10:55:50 AM	Copies	1
User	simpletestuser	Duplex mode	1-sided
Pages	2	Color mode	Color
Account	DEFAULT	Page size	A4
Balance	\$100.00	Cost	\$0.34

Note: You may be able to change the settings of held print jobs on the PaperCut MF Print Release screen before releasing them. For more information, see [6.2 Held print job settings at the device](#).

12. Log out of the device.
13. Log in to the PaperCut MF Admin web interface.
14. Navigate to **Logs**.
15. After printing is completed, verify that **Job Log** page displays the test user’s name, simple test user, in the **User** column and the **Charged To** column:

DATE	USER	CHARGED TO	PRINTER	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Jan 3, 2018 11:27:15 AM	simpletestuser	simpletestuser	device/Library-5	1 (Color: 0)	\$0.05	Prep activities - week 1	A4 (ISO_A4) Duplex: No Grayscale: Yes 38 kB laptop-simpletestuser PostScript	Printed refund edit

16. Log out of the PaperCut MF Admin web interface.

5.2.3 Simple copying

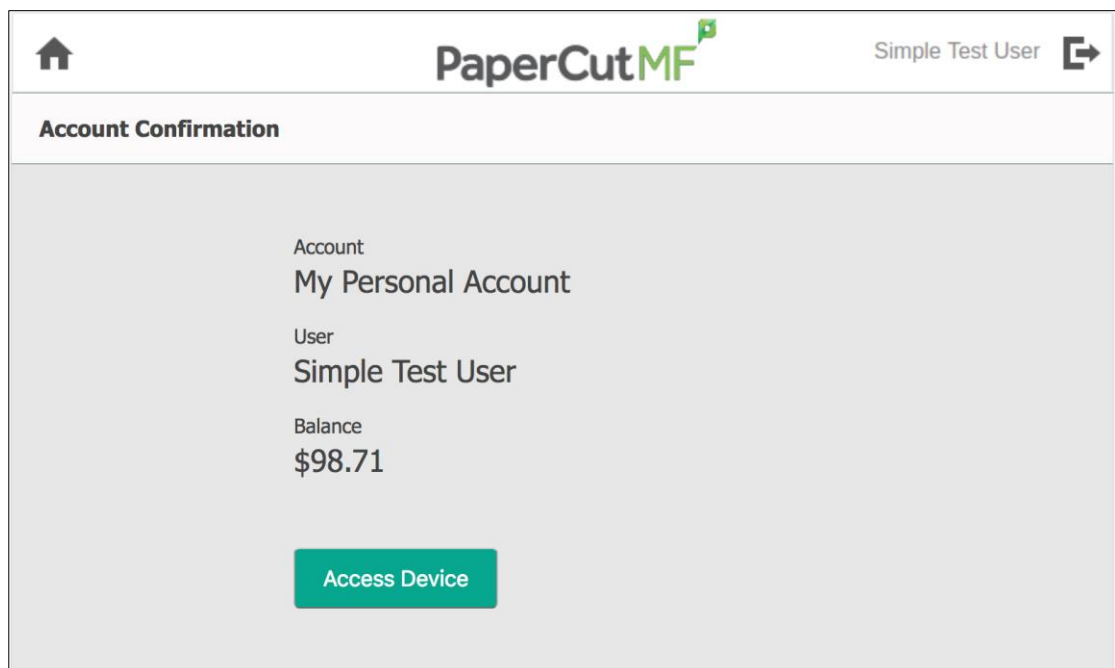
Simple copying does not involve providing the simple test user with a choice of accounts to choose from. Copying is charged to the simple test user’s default My Personal Account.

To test simple copying, ensure the following test preparation requirements are met:

- **Simple test user** - A simple test user is created and configured. For more information, see [5.1 Test preparation: create test users](#) and [5.2.1 Test preparation: configure simple test user](#).
- **Device functions** – The copying function is enabled. To enable the copying function:
 1. Log in to the PaperCut MF Admin web interface.
 2. Navigate to **Devices**.
 3. Select the device being tested.
 4. In the **External Device Settings > Tracking** area, select **Track & control copying**.
 5. Click **Apply**.
 6. Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.

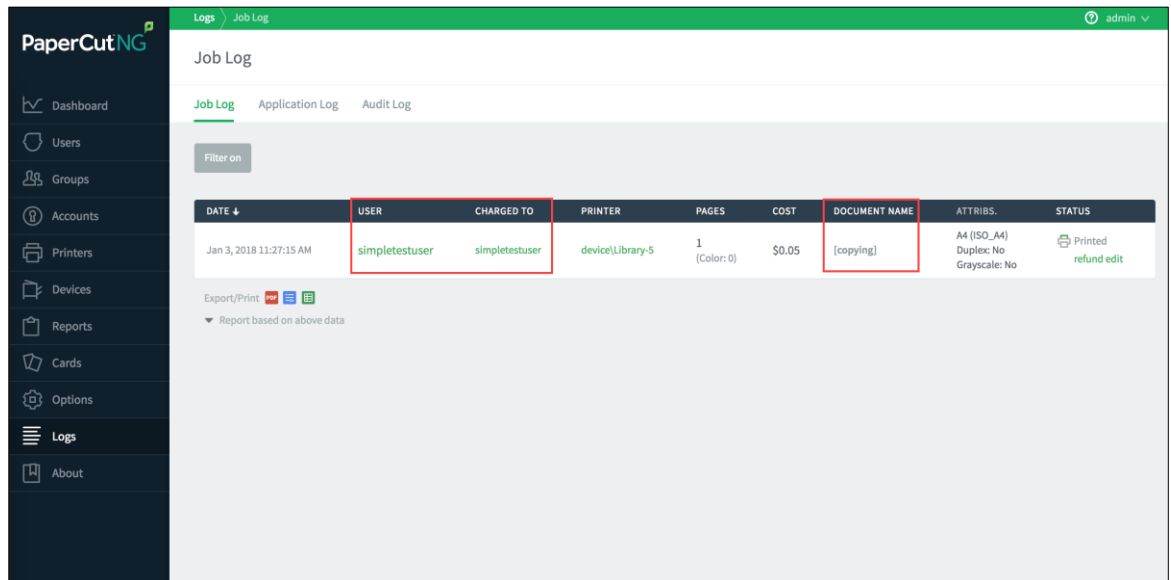
To test simple copying:

1. Log in to the device as the simple test user.
2. Verify that the PaperCut MF Account Confirmation screen does not provide the simple test user with a choice of accounts to choose from, and charges copying to the simple test user's default My Personal Account:



3. Click **Access Device**.
4. Select **Copy**.
5. Complete copying by following the device's workflow.
6. Log out of the device.
7. Log in to the PaperCut MF Admin web interface.
8. Navigate to **Logs**.

- After copying is completed, verify that **Job Log** page displays the test user's name, simple test user, in the **User** column and the **Charged To** column:



- Log out of the PaperCut MF Admin web interface.

5.3 Advanced copying

Advanced copying involves providing the advanced test user with a choice of accounts to choose from. Copying is charged to the account that is selected by the advanced test user.

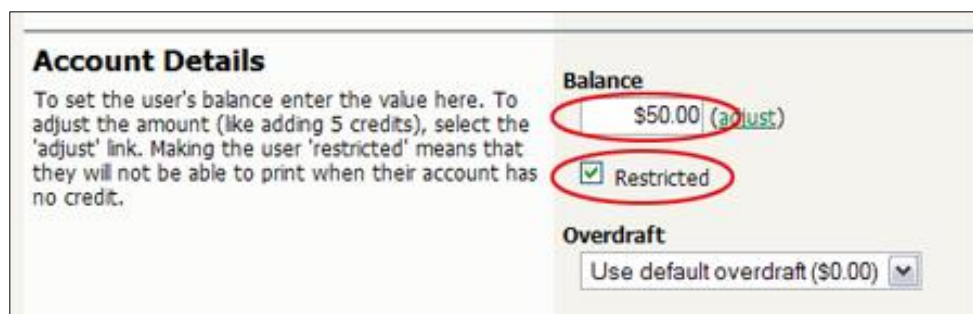
To test advanced copying, ensure the following test preparation requirements are met:

- Advanced test user** – An advanced test user must be created. For more information, see [5.1 Test preparation: create test users](#).

Once created, the advanced test user must be configured.

To configure the advanced test user:

- Log in to the PaperCut MF Admin web interface.
- Navigate to **Users**.
- From the **User List**, select the advanced test user.
- In the **Account Details** area, set the **Balance** to **\$50.00** and select **Restricted**:



- In the **Account Selection** area's **Print account selection**, select **Standard account selection popup** and in **Information to show in popup**, select all the

options:

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

Print account selection
Show the standard account selection popup

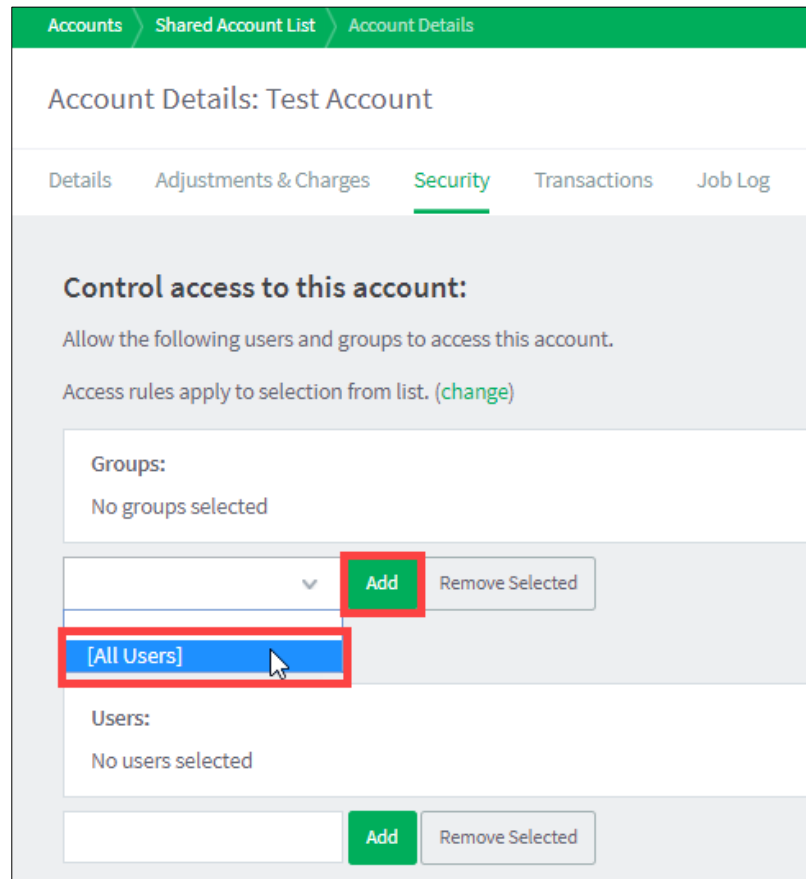
Information to show in popup

- Allow user to charge to their personal account
- Allow user to select shared accounts (from list)
- Allow user to select shared accounts (using PIN/code)

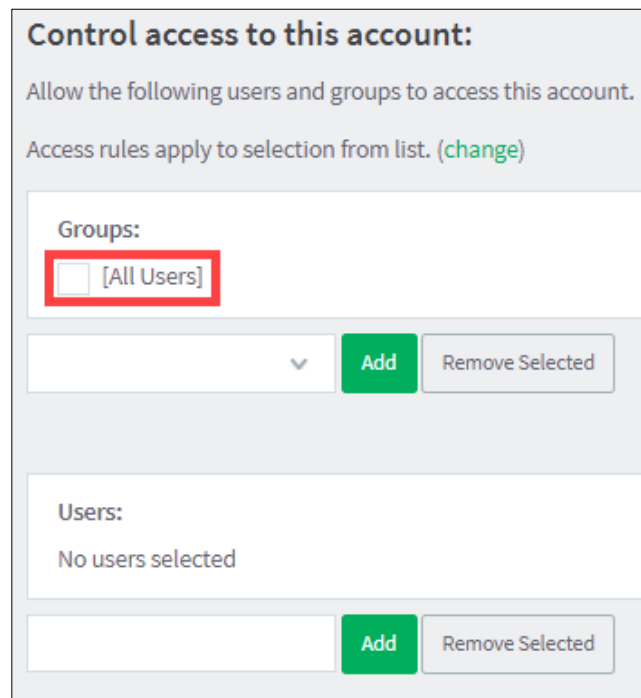
6. Click **Apply**.

- **Device functions** – The copying function is enabled.
To enable the copying function:
 1. Log in to the PaperCut MF Admin web interface.
 2. Navigate to **Devices**.
 3. Select the device being tested.
 4. In the **External Device Settings > Tracking** area, select **Track & control copying**.
 5. Click **Apply**.
 6. Verify that the **Devices > External Device List** displays the device with **Copier** in the **Function** column.
- **Advanced account** – A test account is created.
To create a test account:
 1. Log in to the PaperCut MF Admin web interface.
 2. Navigate to **Accounts**.
 3. Click **Create a new account...**
 4. In the **Details & Balance** area's field **Account Name**, enter the name of the test account (test account).
 5. Click **Apply**.
 6. Verify that the **Accounts > Shared Account List** page displays the test account created.
 7. Click the test account.
 8. Navigate to **Security**.

- 9. In the **Control access to this account > Groups** area, select **[All Users]**; then click **Add**:

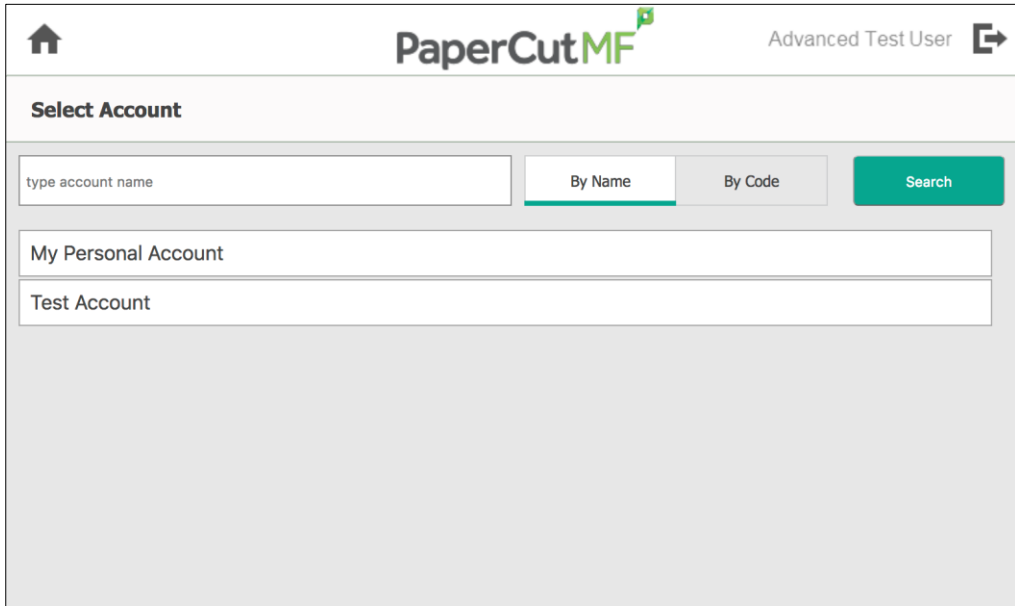


- 10. Verify that the **Control access to this account > Groups** area displays **[All Users]**:

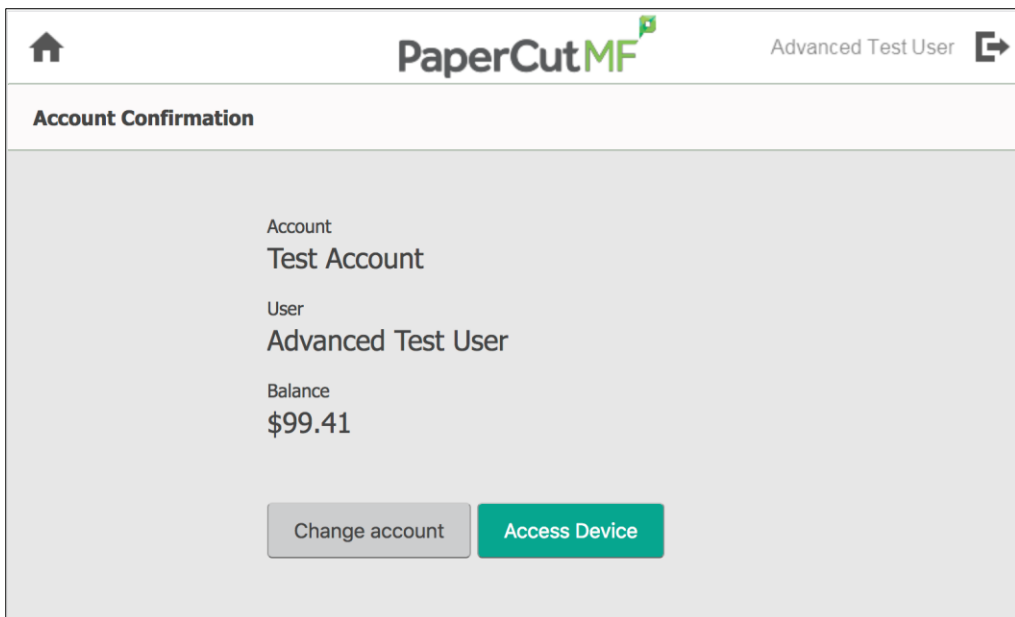


To test advanced copying:

1. Log in to the device as the advanced test user.
2. Verify that the PaperCut MF Select Account screen provides the advanced test user with a choice of accounts to choose from:

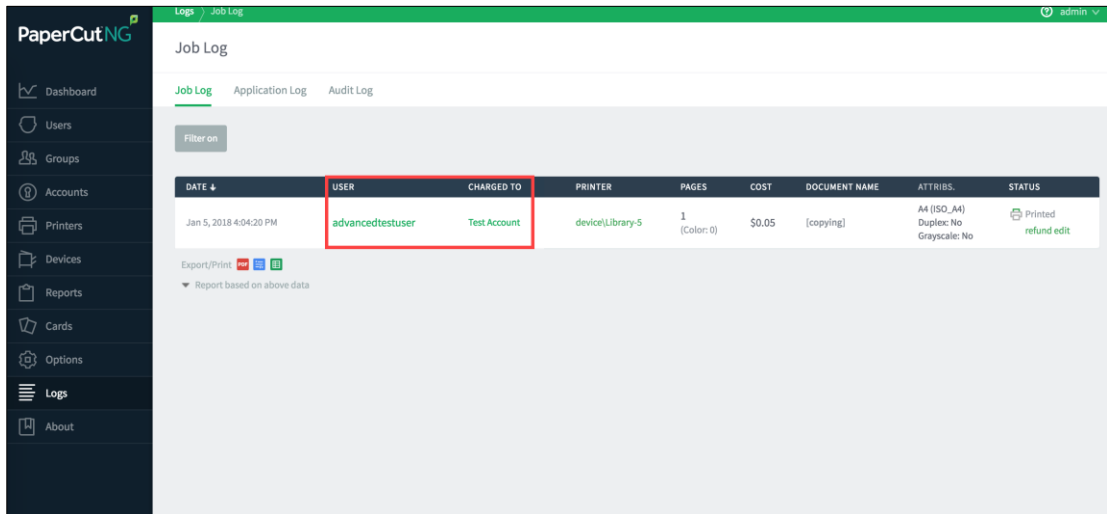


3. Select the relevant account, test account.
4. Verify that the PaperCut MF Account Confirmation screen displays the selected account, test account, but continues to provide the advanced test user with the option of changing the account:



5. Click **Access Device**.
Copying is charged to the account selected by the advanced test user, test account.
6. Select **Copy**.
7. Complete copying by following the device's workflow.
8. Log out of the device.
9. Log in to the PaperCut MF Admin web interface.
10. Navigate to **Logs**.

- After copying is completed, verify that **Job Log** page displays the test user’s name, advanced test user, in the **User** column and the selected account’s name, test account, in the **Charged To** column:



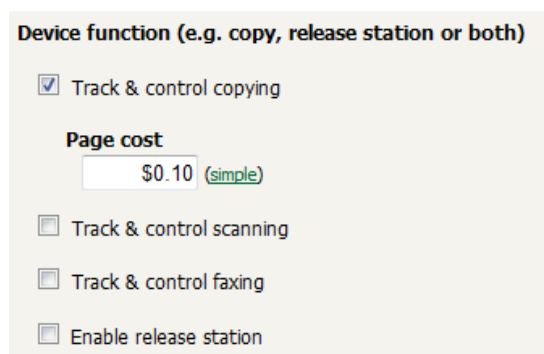
- Log out of the PaperCut MF Admin web interface.

6 Configuration

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

6.1 Device Function

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



Each device function is discussed in the following table.

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

Track & control scanning	The device will track scanning such as scan-to-email or scan-to-file.
Track & control faxing	The device will track the sending of faxes.
Enable release station	The device will act as a print release station.

6.2 Held print job settings at the device

PaperCut MF allows you to configure the following:

- [6.2.1 Held print jobs settings that can be changed at the device](#)
- [6.2.2 Held print jobs settings that can be viewed at the device](#)

6.2.1 Held print jobs settings that can be changed at the device

PaperCut MF allows users to change the settings of held print jobs on the device. Based on the changes made, PaperCut MF shows the updated cost and savings, to give immediate positive feedback to the user, encouraging behavior change.

Users can make the following changes to print settings for multiple jobs on the device:

- **Force grayscale** (from color to grayscale)
- **Force 2-sided** (from 1-sided to 2-sided)

The screenshot shows the PaperCut MF interface. At the top, there is a button labeled 'Access Device', the PaperCut MF logo, and the user name 'Advanced Test User' with an external link icon. Below this is a header bar with a checkbox for 'Select all jobs' and a refresh icon. The main area contains a list of four held print jobs, each with a checkbox, job name, details, time since printing, and a chevron icon:

<input type="checkbox"/>	Prep activities - week 1 1 copy, 2-sided, Grayscale, A4	moments ago	>
<input type="checkbox"/>	Prep activities - week 2 1 copy, 1-sided, Color, A4	4 minutes ago	>
<input type="checkbox"/>	Report template 2 copies, 2-sided, Grayscale, A4	1 hour ago	>
<input type="checkbox"/>	SchoolNewsLetter Template 1 copy, 1-sided, Color, A4	1 day ago	>

At the bottom of the interface, there are two checkboxes: 'Force grayscale' and 'Force 2-sided'. To the right of these are a trash icon and a large teal 'Print' button.

Clicking the chevron of a held print job displays all the settings for the individual job, allowing users to make the following additional changes:

- **Copies**

- **Duplex mode** (from 1-sided to 2-sided)
- **Color mode** (from color to grayscale)
- **Account**

Setting	Value
Time	Jun 15, 2018 1:16:33 PM
User	advanced test user
Pages	1
Account	Test Account
Balance	\$100.00
Copies	1
Duplex mode	1-sided
Color mode	Grayscale
Page size	A4
Cost	\$1.15 Saved \$1.35

Buttons: [Reset to original](#), [Print](#)

If required, you can however, prevent users from being able to change print settings on the device. For more information, see the [PaperCut MF manual](#)

6.2.2 Held print jobs settings that can be viewed at the device

By default, PaperCut MF displays the following print settings for individual jobs on the device:

- **Account**
- **Balance**
- **Cost**

PaperCut MF also displays the total cost for multiple jobs on the device.

If required, you can however, prevent users from being able to view print settings on the device. For more information, see the [PaperCut MF manual](#)

6.3 Authentication Methods

PaperCut MF provides you with several authentication methods to authenticate users when logging in to PaperCut MF on the device.

To access the available authentication methods on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.

The available authenticate methods are in the **Device Details** page's **External Device Settings** area:

Access methods

User authentication

Username and password

Identity number

Swipe card

Guest access

Allow guest/anonymous access

Note: You may use any one or a combination of all the available authentication methods, including the anonymous and guest access authentication methods.

The available authentication methods are:

Authentication Method	Description
Username and password	<p>This is the default authentication method.</p> <p>With this method, users use their domain/network username and password.</p>
Identity number	<p>With this method, users use their ID number. For more information, see the PaperCut MF manual.</p> <p>Require PIN: With this method, users use their id number and the PIN associated with the id number.</p> <p>Note: Users can use an id number with or without a pre-set and associated PIN. If using an id number without a pre-set and associated PIN, users are prompted to set a valid PIN to associate with the id number.</p>
Swipe card	<p>With this method, users use their registered swipe card (e.g. magnetic strip, smart card, RFID). For more information, see the PaperCut MF manual.</p> <p>Require PIN: With this method, users use their registered swipe card and the PIN associated with the card.</p> <p>Note: Users can use a swipe card with or without a pre-set and associated PIN. If using a swipe card without a pre-set and associated PIN, users are prompted to set a valid PIN to associate with the swipe card.</p> <p>Enable self-association with existing user accounts: With this method, users can use a registered swipe card or a new, unregistered swipe card. If</p>

using new, unregistered swipe cards, users are prompted to complete card self-association using their username and password (i.e. associating a new unregistered card with a relevant, valid user account). After card self-association is completed, subsequent use of the registered swipe card does not require users to enter their credentials. You may use the config keys: **ext-device.card-self-association.use-secondary-card-number** and **ext-device.self-association-allowed-card-regex**.

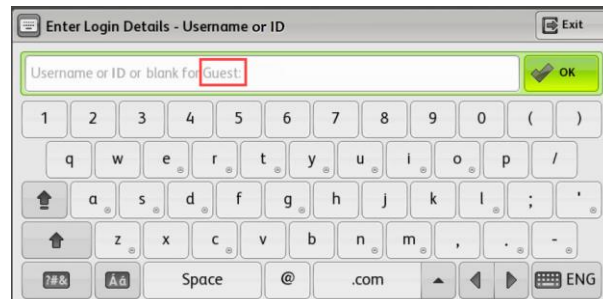
Allow guest/anonymous access

With this method, you may choose to activate **guest** or **anonymous access**, enabling users to be authenticated as guest or anonymous users, as per the user specified in the **Inherit settings from user** field.

Inherit settings from user: Enter the username of the PaperCut MF user's profile that is used while authenticating users as guest or anonymous users on the device.

- **Anonymous access** - Only selecting the **Allow guest/anonymous access** authentication method *without* selecting any other authentication method, activates **Anonymous access**. With this method:
 - A user clicking the **Alternate Login** button or the **keyboard** icon, is authenticated as an anonymous user, as per the user specified in the **Inherit settings from user** field.
 - This anonymous user can view held print jobs belonging to all users.
 - This anonymous user cannot automatically release all jobs on login.
- **Guest access** - Selecting the **Allow guest/anonymous access** authentication method *and also* selecting one or more of the other authentication methods (Username and password, Identity number, Swipe card), activates **Guest access**. With this method:
 - The login screen and available ways for users to log in on the device is based on the other authentication methods selected:
 - If the **Allow guest/anonymous access** authentication method is selected together with only the Swipe card authentication method, then the user can access the device as a guest by clicking the **Alternate Login** button or the **keyboard** icon. This user is then authenticated as a guest user, as per the user specified in the **Inherit settings from user** field.
 - If the **Allow guest/anonymous access** authentication method is selected together with any other authentication method (Username and

password, Identity number, with or without the Swipe card method), then the user is presented with a **Guest** instruction (which you can customize) together with instructions for all other authentication methods selected:



The user can access the device as a guest by clicking the **Ok** button. This user is then authenticated as a guest user, as per the user specified in the **Inherit settings from user** field.

Note: To customize the text of the **Guest** instruction, use the config key **ext-device.xerox.guest-access.label**. For more information, see [7.1 Config Editor](#).

- This guest user is shown the PaperCut MF Account Confirmation screen only if the user profile of the user specified in the **Inherit settings from user** field is entitled with the option of account selection, irrespective of the **External Device Settings > Device Options > Show account confirmation** checkbox setting.

Description of available authentication methods

6.4 Configuring Swipe Card Readers

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

- A typical case is the checksum being reported after the card number, separated by an equals sign, such as in 5235092385=8. PaperCut can handle this case by default; it will extract the number before the equal sign as the card number: 5235092385.
- For some cases, a “regular expression” *may* be required that will filter the card number from the complete string of characters reported by the card reader. Documentation on regular expressions can be found on the Internet, e.g. at www.regular-expressions.info.
 - The regular expression must be fashioned so that the card number is returned as the first match group.

- Usually one regular expression will be used for all the devices managed by PaperCut; this must be entered in the “Config editor (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: `{\d19}`
 - Extract the digits from between the two “=” characters in “123453=292929=1221”: `\d*=(\d*)=\d*`

6.5 Account selection

The PaperCut MF Select Account screen on the device allows users to select an account via any one of the following ways:

- [6.5.1 By name and by code](#)
- [6.5.2 By name](#)
- [6.5.3 By code](#)

This is based on a user’s Account Selection setting on the PaperCut MF Admin web interface. To this on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Users**.
3. From the **User List**, select the user.
4. In the **Account Selection** area’s **Print account selection**, select **Standard account selection popup** and in **Information to show in popup**, select all the options:

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

Print account selection
Show the standard account selection popup

Information to show in popup

- Allow user to charge to their personal account
- Allow user to select shared accounts (from list)
- Allow user to select shared accounts (using PIN/code)

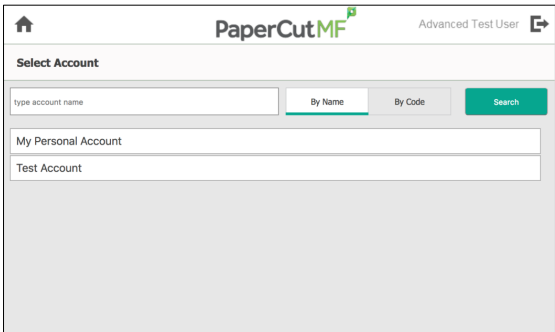
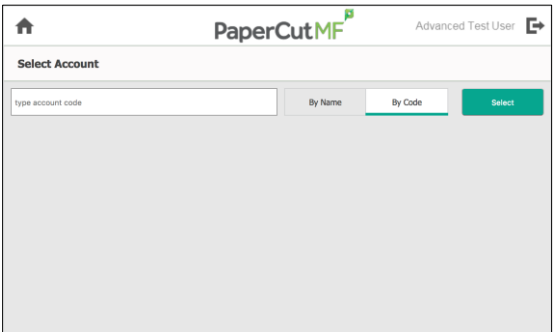
6.5.1 By name and by code

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to either of the following, the PaperCut MF Select Account screen displays both methods of selecting accounts – by name and by code:

- **Show the advanced account selection popup**, or

- **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (from list)** and **Allow user to select shared accounts (using PIN/code)**

Note: To customize which of the two tabs is open by default on the PaperCut MF Select Account screen, use the config key `ext-device.xerox.initial-account-tab`. For more information, see [7.1 Config Editor](#).

By Name	By Code
<p>Users select the relevant shared account by scrolling through a list of all applicable shared accounts (maximum of 500, with a scroll bar) or by searching for the shared account using the account's name.</p> <p>Note: The user's My Personal Account and the Default Shared Account (if set) is always displayed.</p>	<p>Users select the relevant shared account by using the shared account's code.</p> <p>Note: The user's My Personal Account and the Default Shared Account (if set) is not displayed.</p>
	

6.5.2 By name

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (from list)**, the PaperCut MF Select Account screen displays only one method of selecting accounts – by name. Users select the relevant shared account by scrolling through a list of all applicable shared accounts (maximum of 500, with a scroll bar) or by searching for the shared account using the account's name.

Note: The user’s My Personal Account and the Default Shared Account (if set) is always displayed.

The screenshot shows the 'Select Account' interface. At the top, there is a home icon, the 'PaperCutMF' logo, and the text 'Advanced Test User' with an external link icon. Below this is a search bar with the placeholder text 'type account name' and a green 'Search' button. A dropdown menu is open, showing two options: 'My Personal Account' and 'Test Account'.

6.5.3 By code

For users who on the PaperCut MF Admin web interface (**Users > Details**) have **Account Selection** set to **Show the standard account selection popup** and **Information to show in popup** set to **Allow user to select shared accounts (using PIN/code)**, the PaperCut MF Select Account screen displays only one method of selecting accounts – by code. Users select the relevant shared account by using the shared account’s code.

Note: The user’s My Personal Account and the Default Shared Account (if set) is always displayed.

The screenshot shows the 'Select Account' interface for search by code. At the top, there is a home icon, the 'PaperCutMF' logo, and the text 'Advanced Test User' with an external link icon. Below this is a search bar with the placeholder text 'type account code' and a green 'Select' button. In the center of the screen, the word 'Or' is displayed. Below this, a dropdown menu is open, showing one option: 'My Personal Account'.

6.6 Single Sign On (SSO)

No further configuration is required as PaperCut passes all the known information about the logged in user to the MFP at the time of login such as the Full Name, email address, and more. This information can then be used by other components on the MFP (or possibly other 3rd party applications).

One example is that when you use the scanner functionality, the MFP can use your email address, provided by PaperCut, to simplify scan-to-me style work-flows.

7 Advanced Configuration

7.1 Config Editor

The common configuration options for a device in PaperCut are available on the device's 'Summary' tab, and are discussed in more detail in the Configuration section. This section covers the more advanced or less common configuration options, which are available via the 'Advanced Config' tab.

Config name	Description
ext-device.card-self-association.use-secondary-card-number	<p>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.</p> <p>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.</p>
ext-device.xerox.login-instruction	<p>Customize the text that appears on the PaperCut MF Login screen. For example, instructions to help users log in to PaperCut MF on the device.</p> <p>This is a device-specific config key.</p> <p>Values: Any text, DEFAULT, DONOTSET (text specified in the device's web interface)</p> <p>Default: DEFAULT (device-specific PaperCut MF text based on Authentication methods selected)</p> <p>Note: To add a line break, use \n. For example, PaperCut Software\nSwipe your card to log in.</p> <p>IMPORTANT: It is recommended that you use only ASCII characters because of the limited support for non-ASCII characters.</p>
ext-device.xerox.job-download-after-login-period-secs	<p>The number of seconds between PaperCut downloading/polling the device job logs after the user is logged in. The default for this is every 10 seconds. The minimum this can be set to is 5 seconds.</p>

	Default: DEFAULT (which allows PaperCut to choose the most appropriate time – usually 10 seconds).
ext-device.xerox.auth-user-prefix	<p>When user's login to the Xerox their credentials like username (and password if provided) are passed to the Xerox device by PaperCut. This allows the device to use these credentials for other authentication. E.g. To authenticate the use when using the "Scan to Home" features.</p> <p>In some environments, the username must be prefixed with the windows domain for this to work properly. This setting allows the domain to be prefixed to the username so that the user does not need to enter it manually.</p> <p>For example, if this setting is set to: "DOMAIN\" and the user named "john" logs in, PaperCut will pass the username "DOMAIN\john" to the Xerox.</p>
ext-device.xerox.card.magstripe-track-no	<p>When a USB Magstripe card reader is used, the card data can be found on one of 3 tracks. Typically, the track of interest is track number 2. This configuration parameter specifies a comma separated list of track numbers to look at in order to retrieve the card data. For example, if the list was: 2, 3 then it would look to see if there was data for track 2 and if there wasn't then it would look to see if there was data for track 3. If it can't find any valid track data, then it will show an error message on the Xerox Panel and a more detailed message in the logs. Note: Prior to PaperCut 13.4, this list can only contain one value.</p> <p>Default: 2 (by default only look at the data associated with track 2)</p>
ext-device.xerox.locale-override	<p>Specify a language tag adhere to the supported locale list to force the locale setting for use on the device.</p> <p>The locale is determined by the following priority sequence:</p> <ol style="list-style-type: none">1. ext-device.xerox.locale-override setting2. The language set on the Xerox device3. The locale set on the PaperCut server (system.default-locale config key)4. The default locale configured on the operating system running the PaperCut server
ext-device.xerox.use-job-owner	<p>Specify the source of the user Id used to identify the owner of a job from the Xerox Job Logs:</p> <ul style="list-style-type: none">• Y—use the Job-Owner field to determine the user Id.• N—use the Accounting-User-Id field to determine the user Id.

ext-device.xerox.initial-account-tab	<p>Customize which of the two tabs is open by default on the PaperCut MF Select Account screen.</p> <p>This is a device-specific config key.</p> <p>Values: List (default open tab is By Name), Code (default open tab is By Code)</p> <p>Default: List</p> <p>Note: This is applicable only to users who on the PaperCut MF Admin web interface have Account Selected set to:</p> <ul style="list-style-type: none">• Show the advanced account selection popup, or• Show the standard account selection popup and Information to show in popup set to Allow user to select shared accounts (from list) and Allow user to select shared accounts (using PIN/code) <p>For more information, see 6.5 Account selection.</p>
ext-device.xerox.release-show-cost	<p>Toggle the display of the cost of held print jobs on the PaperCut MF Print Release screens on the device.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none">• Values: Y, N• Default: Y <p>Note: Setting this to N also hides the account balance and does not display the savings based on other changes made to held print job settings. For more information, see 6.2 Held print job settings at the device.</p>
ext-device.xerox.select-account	<p>Specify whether to support the Account Selection app on the MFP and display of the Account Selection Page. Values: Y, N. Default: Y</p> <p>If set to N, the Account Selection App will not be registered on the MFP and therefore no Account Selection icon will be shown on the panel. Instead, account selection will be done during the Secure Access login workflow. A reason to set this to N is to be able to force the user to choose an account in the cases of EIP 1.5 devices or EIP 2.0+ devices that want to use the Job Assembly feature.</p> <p>On EIP 3.0+ devices:</p> <p>This key is not used anymore, as there is a single app registered on the MFP called "PaperCut MF"</p>
ext-device.xerox.require-account-selection	<p>Specify whether to always stop the user performing a copier job until they select an account in the Account Selection dialog. Values: Y, N. Default: N.</p>

	<p>If set to N, then it will only force account selection if the user is not allowed to charge to their personal account and they haven't chosen an account yet.</p> <p>If set to Y, then the user must choose an account otherwise they won't be able to perform a job.</p>
<code>ext-device.xerox.account-cache-timeout-mins</code>	<p>On EIP1.5 devices: Sets the number of minutes after an account is selected (in the account selection application) that the shared account for a user is held in memory. The default is 24 hours</p> <p>On EIP2+ devices: Sets the number of minutes after a job is initiated that the shared account for a job is held in memory. The default is 30 minutes.</p>
<code>ext-device.xerox.enable-preauth</code>	<p>Relevant to EIP 2.0+ devices only.</p> <p>Specify whether PaperCut should enable or disable the Accounting Workflow preauthorization on the device for the different types of jobs. This is required for Zero Stop to work. Values: Y, N. Default: Y.</p> <p>If set to N, then it will change the preauthorization from "Pre-authorization and Capture Usage" to "Capture Usage". This can be done so that the Job Assembly feature is enabled on Xerox. Zero Stop will not work and the Account Selection app will no longer be available.</p>
<code>ext-device.xerox.configure-preauth-and-prompts</code>	<p>Relevant to EIP 2.0+ devices only.</p> <p>Specify whether PaperCut should configure the Accounting Workflow and Prompts on the device for full PaperCut functionality. Values: Y, N. Default: Y.</p> <p>If set to N – it is your responsibility to configure the MFP Accounting Workflow and User Accounting Prompts to suit your needs. Note that normal PaperCut job control may not work as expected. In particular, Zero Stop may not work and the Account Selection app will no longer be available (account selection via Secure Access workflow will be enabled instead).</p>
<code>ext-device.xerox.send-users-email-address-to-device</code>	<p>Specify whether or not the user's PaperCut MF email address is sent to the device on login.</p> <p>Values: Y, N. Default: Y.</p> <p>If set to Y, the PaperCut MF email address is sent to the device on login. If it is set to N, then the email address is not sent to the device, which means the device does not populate any addresses with the PaperCut MF email for that user.</p>

ext-device.xerox.swipe-to-logout	<p>Specify whether swiping a card when a user is logged in will log them out or be ignored.</p> <p>Values: Y, N. Default: Y.</p> <p>If set to N, then when a user is logged in and they swipe their card, they will no longer be logged out and the swipe will be ignored.</p>
ext-device.xerox.release-app-label	<p>Customize the text of the PaperCut MF Print Release icon that appears on the device.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none">• Values: Any text, DEFAULT• Default: DEFAULT (Home) <p>Note: This is applicable if the device is enabled with only Print Release. As a result, it overrides the config key ext-device.xerox.release-app-label.</p>
ext-device.xerox.use-ssl-for-apps	<p>Determines whether "https" or "http" is used for the URLs of the PaperCut Account Selection App and the PaperCut Print Release App. Set this to Y to use "https" (i.e. "SSL", secure). Set this to N to use "http" (i.e. "not SSL", not secure).</p> <p>Values: Y, N. Default: DEFAULT (N)</p> <p>Non-secure setting of N maybe required when looking at packet captures for diagnosing issues involved with using these apps.</p> <p>Secure setting of Y is recommended if there are concerns about the privacy of the chosen Shared Account and/or Print Job Titles to release for a user.</p>
ext-device.xerox.always-use-ip-address-for-secure-access	<p>Determines whether an IP address or a hostname is to be used for Secure Access configuration. Set this to Y to use an IP address for Secure Access configuration. Set this to N to allow for a hostname to be used for Secure Access on some Xerox devices that support it.</p> <p>Values: Y, N. Default: Y</p> <p>It is recommended that this is not modified.</p>
ext-device.xerox.track-scan-to-ifax-as-fax-jobs	<p>Track scan to fax jobs as scan jobs or fax jobs.</p> <p>Set this to Y to track as fax jobs.</p> <p>Set this to DEFAULT to track as scan jobs.</p> <p>Values: Y, N, DEFAULT</p> <p>Default: DEFAULT (N)</p>

ext-device.xerox.enable-secure-access	<p>Automatically enable Secure Access configuration. Set this to Y to automatically enable Secure Access configuration via SNMP. Set this to N to opt to manually enable Secure Access configuration via the device's web admin page.</p> <p>Values: Y, N</p> <p>Default: Y (automatically enable Secure Access)</p>
ext-device.xerox.lock-device	<p>Configure PaperCut to honor or automatically re-set the device-level user authentication permissions.</p> <p>Note: Avoid modifying this setting for VersaLink devices.</p> <p>Values: Y, N. Default: Y</p> <p>Setting this to 'N' will honor device-level user authentication permissions and not automatically reset them.</p> <p>Setting this to 'Y' will automatically re-set device-level user authentication permissions and will require user authentication for all device functions.</p>

ext-device.xerox.header.color	<p>The background color of the header.</p> <p>Values: Any valid HTML color name or hexadecimal notation of the color (#RRGGBB); where “RR” is the red component, “GG” is the green component and “BB” is the blue component.</p> <p>Default: DEFAULT (#fbfafa)</p> <p>See Customizing the header logo and colors</p>
ext-device.xerox.header.textcolor	<p>The color of the text in the header.</p> <p>Values: Any valid HTML color name or hexadecimal notation of the color (#RRGGBB); where “RR” is the red component, “GG” is the green component and “BB” is the blue component.</p> <p>Default: DEFAULT (#888888)</p> <p>See Customizing the header logo and colors</p>
ext-device.xerox.welcome-text	<p>The text displayed on the information bar of the PaperCut Home screen. Use this text to provide specific information about logging in to the device.</p> <p>Default: DEFAULT (Welcome, <username>).</p> <p>Note: This setting is overridden by the ext-device.home-screen.show-balance setting for users who have an auto-chargeable account.</p>
ext-device.inactivity-timeout-secs	<p>PaperCut MF timeout: Customize the interval of time (seconds) after which a user who is detected as being idle on PaperCut MF is automatically logged out.</p> <p>This is a device-specific config key.</p> <ul style="list-style-type: none">• Values: Any positive number (seconds)• Default: 60 (seconds) <p>Note: This comes into effect only if it is lower than the value of the device’s timeout. However, if it is higher, then it is overridden by the lower value of the device’s timeout.</p>
ext-device.xerox.timeout.scan-prompt-send.secs	<p>PaperCut MF Scan More or Finish timeout: Customize the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan More or Finish (with the three buttons – Scan next page, Scan new document, Finish) screen is automatically taken to the PaperCut MF Scan Complete (with scan completed or failed status). The process of sending the completed scan job to the user (scan transfer) is also automatically initiated, and the user is logged out.</p> <p>This is a device-specific config key.</p>

-
- Values: Any positive integer, DEFAULT
 - Default: DEFAULT (30 seconds)

Note: This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout.

ext-
device.xerox.timeout.complete
-scan-job.secs

PaperCut MF Scan Complete timeout: Customize the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Completes screen (with scan completed or failed status), is automatically logged out.

This is a device-specific config key.

- Values: Any positive integer, DEFAULT
- Default: DEFAULT (5 seconds)

Note: This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout.

ext-
device.xerox.scan.prompt.chec
kbox.checked

Customize the default setting of the PaperCut MF Scan screens' **Prompt for more pages** checkbox (checked or unchecked) and the display of the PaperCut MF Scan More or Finish (with the three buttons – **Scan next page, Scan new document, Finish**) screen.

This is a device-specific config key.

- Values: Y (checked by default; can be changed by the user), N (unchecked by default; can be changed by the user)
- Default: Y

Note:

- A checked **Prompt for more pages** checkbox displays the PaperCut MF Scan More or Finish (with the three buttons – **Scan next page, Scan new document, Finish**) screen, to provide users with the option of adding more pages to the scan job.
- An unchecked **Prompt for more pages** checkbox causes the PaperCut MF Scan More or Finish (with the three buttons – **Scan next page, Scan new document, Finish**) screen to not be displayed; the process of sending the completed scan job to the user (scan transfer) is automatically initiated; only the PaperCut MF Scan Complete (with scan completed or failed status) screen is displayed. As a result, users are not provided with the option of adding more pages to the scan job or starting a new scan job.

ext-device.xerox.force-widget-keyboard	<p>Configure which type of keyboard is to be used - Xerox native device keyboard or Xerox widget keyboard.</p> <p>Note: This setting is only available for Xerox devices with the firmware EIP 3.0 or higher.</p> <p>Values: Y, N</p> <p>Default: N</p> <p>Setting this to N, uses the Xerox native device keyboard.</p> <p>Setting this to Y, uses the Xerox widget keyboard.</p>
ext-device.block-release-on-error.snmp-error-list	<p>The error types that can cause a device to become a device in error, blocking the release of print jobs on the device. The error types include: lowPaper, noPaper, lowToner, noToner, doorOpen, jammed, offline, serviceRequested, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputNearFull, outputFull, inputTrayEmpty, overduePreventMaint</p> <p>Values: Any one or a comma-separated combination of the above error types.</p> <p>Default: DEFAULT (noPaper, doorOpen, jammed, offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull)</p> <p>Note: Some Xerox devices may return the error type inputTrayEmpty when the device is out of paper, instead of using the error type noPaper. For these devices, ensure NOT to use the default value. Manually enter all the required error types, including the error type inputTrayEmpty.</p>
ext-device.block-release-on-error.snmp-byte-order-mode	<p>When a device is in error, the byte order used by the device to return the SNMP status to the PaperCut MF embedded application. This is applicable to devices that can return SNMP status in either REVERSE or FORWARD byte orders.</p> <p>Values: FORWARD, REVERSE, DEFAULT</p> <p>Default: DEFAULT (FORWARD)</p> <p>Setting this to Default is recommended when the byte order used by the device to return the SNMP status to the PaperCut MF embedded application, is unknown.</p> <p>Note: If the device reports incorrect errors, override the default setting and manually set the value to REVERSE. If the device continues to report incorrect errors, contact support@papercut.com.</p> <p>Setting this to FORWARD or REVERSE, is recommended when the byte order used by the device to return the SNMP status to the PaperCut MF embedded application, is known.</p>

ext-device.home-screen.show-balance	<p>Configure the PaperCut Home screen to display the following based on the type of user (restricted or unrestricted):</p> <ul style="list-style-type: none">• auto-chargeable account details AND balance on the PaperCut Home screen – for restricted users• only auto-chargeable account details on the PaperCut Home screen – for unrestricted users <p>This is applicable only to users who have either of the following Account Selection options enabled on the Admin web interface (Users > User List > User Details):</p> <ul style="list-style-type: none">• Automatically charge to personal account OR• Automatically charge to a single shared account <p>This key can set in Options > Config editor (advanced).</p> <p>Values: Y, N, Default</p> <p>Default: DEFAULT (N)</p> <p>Setting this to Y displays the auto-chargeable account and balance, based on the type of user (restricted or unrestricted).</p> <p>Note: This overrides the ext-device.xerox.welcome-text config key.</p> <p>Note: If the user has print jobs waiting to be released, then the PaperCut Home screen displays only the print jobs waiting to be released. After the user has actioned the print jobs waiting to be released, the PaperCut Home screen reverts to the display based on the type of user (restricted or unrestricted) as per the config key setting.</p>
ext-device.xerox.show-release-on-login	<p>Configure the workflow for Xerox devices with the firmware below EIP 3.0, to have PaperCut MF as the default application after login, and to display the Print Release screen.</p> <p>Note: This setting is only available for Xerox devices with the firmware below EIP 3.0. For Xerox devices with the firmware EIP 3.0 or above, see ext-device.xerox.register-papercut-as-default-app (which defaults to the current key's value).</p> <p>Values: Y, N</p> <p>Default: Y</p> <p>Setting this to Y – makes PaperCut MF the default application after login, and displays the Print Release screen.</p> <p>Setting this to N – makes the native device the default application after login. Users must press the Print Release button to access the Print Release screen.</p>
ext-device.xerox.select-account-on-login	<p>Configure the workflow for Xerox devices with the firmware below EIP 3.0, to have PaperCut MF as the default application after login, and to display the Select Account screen.</p>

Note: This setting is only available for Xerox devices with the firmware below EIP 3.0. For Xerox devices with the firmware EIP 3.0 or above, see `ext-device.xerox.register-papercut-as-default-app`.

Values: Y, N

Default: Y

Setting this to Y – makes PaperCut MF the default application after login, and displays the Select Account screen.

Setting this to N – makes the native device the default application after login. Users must press the **Select Account** button to access the Select Account screen.

`ext-device.xerox.register-papercut-as-default-app`

Configure the workflow for Xerox devices with the firmware EIP 3.0 or above, to have PaperCut MF as the default application after login.

Note: This setting is only available for Xerox devices with the firmware EIP 3.0 or above. For Xerox devices with the firmware below EIP 3.0, see `ext-device.xerox.show-release-on-login`.

Values: Y, N

Default: (Y or N based on the value of `ext-device.xerox.show-release-on-login`)

Setting this to Y – makes PaperCut MF the default application after login. Any one of the following screens is displayed, based on other settings:

- The PaperCut Home screen OR
- The PaperCut Print Release screen OR
- The PaperCut Select Account screen OR
- The PaperCut Account Confirmation screen OR
- the native device functions screen

Setting this to N – makes the native device the default application after login. Any one of the following screens is displayed, based on other settings:

- The PaperCut Select Account screen OR
- The PaperCut Account Confirmation screen OR
- the native device functions screen

`ext-device.home-screen.force-show`

After accessing PaperCut MF on the device, configure the workflow to display the PaperCut MF Home screen, irrespective of whether or not Integrated Scanning is enabled and irrespective of whether or not print jobs are waiting to be released.

Set this global config key in the PaperCut MF Admin web interface: Options > Config editor (advanced).

	Values: Y, N Default: N
ext-device.xerox.skip-release-screen-when-no-jobs	<p>After accessing PaperCut MF on the device, configure the workflow to suppress the PaperCut MF Home screen, when Integrated Scanning is not enabled and when there are no print jobs waiting to be released.</p> <p>Values: Y, N Default: Y</p> <p>Note:</p> <ul style="list-style-type: none">Setting this to Y, suppresses the PaperCut MF Home screen. Any one of the following screens is displayed, based on other settings:<ul style="list-style-type: none">The PaperCut Select Account screen ORThe PaperCut Account Confirmation screen ORthe native device functions screen<p>This is recommended only if the device is used more for copying rather than printing.</p>Setting this to N, displays the PaperCut MF Home screen. This is recommended if the device is used for all functions (printing, scanning, copying).
enable-usb-print	<p>Toggle USB printing.</p> <p>Values: Y, N Default: Y</p> <p>Setting this to Y, enables USB printing when either of the following conditions are also met:</p> <ul style="list-style-type: none">Either, copy jobs are not tracked on the device,Or, if copy jobs are tracked on the device, the user has sufficient credit to perform a copy job <p>Setting this to N, disables USB printing.</p>
ext-device.xerox.integrated-scan-job-compression	<p>(Available for EIP 4+ devices only). Set the compression rate for Integrated Scanning files.</p> <p>Values:</p> <ul style="list-style-type: none">HIGHMEDIUMLOW

- NONE—no compression is applied to PDF documents. However, for JPG and TIFF files, MEDIUM compression is applied.

Default: MEDIUM

ext-device.xerox.home-app-label

Customize the text of the **PaperCut MF Home** icon that appears on the device.

This is a device-specific config key.

- Values: Any text, DEFAULT
- Default: DEFAULT (Home)

Note: This config key is overridden by the config key **ext-device.xerox.release-app-label**, if the device is only enabled with Print Release.

ext-device.xerox.guest-access.label

Customize the text of the **Guest** instruction that appears on the login screen.

This is a device-specific config key.

Values: Any text, DEFAULT

Default: DEFAULT (Guest)

Note: This is applicable only if guest access is activated (the **Allow guest/anonymous access** authentication method is selected and at least Username and password or Identity number is also selected). For more information, see [6.3 Authentication Methods](#).

ext-device.xerox.support-switch-mode

Configure the device's Home screen to display only PaperCut MF applications and hide non-PaperCut MF applications, in order to prevent the device's Home screen from freezing upon login.

This is a device-specific config key.

- Values: Y (display both PaperCut MF and non-PaperCut MF applications, which could cause the device to freeze), N (display only PaperCut MF applications, which prevents the device from freezing)
- Default: N

Note: This is only applicable to the following EIP 1.0+, EIP 1.5+ switch mode devices:

- WorkCentre 232/238, 245/255, 265/275, 5135/5150, 5222/25/30/25A/30A, 5632/38/45/55/65/75/87, 7120/7125, 7232/7242, 57xx
- WorkCentre Pro 232/238, 245/255, 265/275
- WorkCentre Bookmark 40&55
- 3635 MFP

ext-device.xerox.dmp-device-charge-account-by-start-time

EIP 1.5 DMP devices with shared account selection: Configure PaperCut MF to accurately track, charge and log jobs.

This is a device-specific config key.

- Values: Y (DMP devices), N (non-DMP devices)
- Default: N

Note: Setting this to Y – is required only if:

- the device is an EIP 1.5 DMP-based device, and
- shared account selection is configured.

ext-device.xerox.snmpv2.set-community-name

If you want PaperCut MF to use SNMP v2c and it is also enabled on the device's web interface, then ensure this is the same as the device web interface's **SET Community Name**.

This is a device-specific config key.

- Values: same as **SET Community Name**, private
- Default: private

For more information, see [4.4.4 SNMP version](#).

ext-device.xerox.snmp-v3-auth-password

If you want PaperCut MF to use SNMP v3 and it is also enabled on the device's web interface, then ensure this is the same as the device web interface's **Authentication Password**.

This is a device-specific config key.

- Values: same as the device web interface's **Authentication Password**.
- Default: same as the PaperCut MF Admin web interface's **SNMP v3 authentication password**.

For more information, see [4.4.4 SNMP version](#).

ext-device.xerox.snmp-v3-privacy-password

If you want PaperCut MF to use SNMP v3 and it is also enabled on the device's web interface, then ensure this is the same as the device web interface's **Privacy Password / Encryption Password**.

This is a device-specific config key.

- Values: same as the device web interface's **Privacy Password / Encryption Password**.
- Default: same as the PaperCut MF Admin web interface's **SNMP v3 privacy password**.

For more information, see [4.4.4 SNMP version](#).

ext-device.xerox.snmp-v3-auth-username

If you want PaperCut MF to use SNMP v3 and it is also enabled on the device's web interface, then ensure this is the same as the

device web interface's **SNMP v3 Authentication Username/ Security Name**.

This is a device-specific config key.

- Values: same as the device web interface's **SNMP v3 Authentication Username/ Security Name**, Xadmin
- Default: Xadmin

For more information, see [4.4.4 SNMP version](#)

7.2 Customizing the header logo and colors

The header logo, the header background color, and the header text color appearing on all the screens of the embedded application can be customized.

To customize the header logo:

- Create a 24bit PNG image of the logo, which is 230 pixels wide and 55 pixels high.
- Save the image with the filename "logo.png" in the following PaperCut application directory and subdirectory:
`[PaperCut Install Location]\server\custom\web\device\xerox\1.5\`
Create the subdirectory if necessary.

To customize the header background color, and the header text color, see the Config Editor for more information about configuring the following:

- ext-device.xerox.header.color
- ext-device.xerox.header.textcolor

Note: Any customizations made (header logo, header background color, header text color) are globally applied across all the embedded application screens, on all Xerox devices running firmware EIP 3.0 or higher. Customizations made are not applied to other Xerox devices on your network.

7.3 Setting an explicit PaperCut Server Network Address

The copier connects to the PaperCut server to validate user credentials, display print jobs for release, etc. The device makes inbound network connections to the PaperCut server using the network address of the PaperCut server. By default PaperCut will use the server's IP address (if the server has multiple IPs (i.e. multi-homed) then PaperCut will select one of them), but on some networks this address may not be publicly accessible from other parts of the network.

If the PaperCut server has a "public" IP address or DNS name then this can be used instead, which allows the copiers to use the "public" network address instead of the IP address that PaperCut detects. To do this:

1. Log into PaperCut MF
2. Go to the "Options" tab.
3. Select "Config Editor (advanced)", from the action links on the left.
4. Find the "system.network-address" setting.
5. Enter the public network address for the PaperCut server.
6. Press the "Update" button next to the setting and confirm the setting is updated.

When connecting devices to a PaperCut site server, you can configure the sites' "Network address used by devices":

1. Login to PaperCut MF.
2. Go to the "Sites" tab.
3. Select the site to edit.
4. Change the "Network address used by devices".
5. Save the site details.

To have either of these changes take effect immediately, restart the PaperCut Application Server service (i.e. on Windows use: Control Panel->Admin Tools->Services).

8 Known Limitations and Security

The Xerox environment has a number of limitations, impacting functionality and security. The limitations differ between various EIP device versions.

8.1 EIP 1.5 device limitations summary

EIP 1.5 devices do not have the Job Limits feature (unlike EIP 2.0+ devices), and this affects the following:

- There is no Zero Stop capability.

If the EIP 1.5 device is using the Account Selection App (which it will by default):

- It cannot force a user to choose a shared account
- It cannot stop a user from logging in without sufficient balance (if they can choose an account) because we don't know what account they will choose at login time

If the EIP 1.5 device is not using the Account Selection App (by setting *ext-device.xerox.select-account* to "N" or if the account selection options for users don't allow the user to select an account):

- we *can* stop the user from logging into the device without sufficient balance
- *BUT* we then cannot allow free scanning or free faxing in this case

8.1.1 No Zero Stop for EIP 1.5 devices

PaperCut implements Zero Stop to prevent users from overrunning their available credit.

Zero Stop works using the Job Limits feature Xerox introduced in EIP 2.0+. Each job is pre-authorized with the PaperCut server, which determines whether or not the job should proceed based on the cost and the associated account balance. When initiating each job, the Xerox panel shows an "authorizing the job" message. If PaperCut does not authorize the job, an error message is displayed and the job does not start.

- Zero Stop is currently supported only for copy and scan jobs and is only available for EIP 2.0+ devices.
- Zero Stop is not supported for fax or USB printing.

- Some early firmware versions do not support Zero Stop for scanning either. (See Section 8, Known Limitations and Security.)

Xerox EIP 1.5 devices (e.g. Xerox 5325) do not support Zero Stop and the ability to stop a job part way through because of insufficient funds. However, if after the job is completed and retrieved from the MFP and the user is out of credit, the user will be logged off the device.

8.1.1.1 No Zero Stop for USB Printing

While tracking USB print jobs as copy jobs is available for Xerox EIP 1.5+ devices, Zero Stop is not available. That means that users can complete a USB print job and possibly incur an overdraft in their accounts. However, USB printing is not available (i.e. the **Print From...** button is not displayed) for restricted users that have an insufficient credit balance for a single page copy job.

8.1.2 Less automatic configuration on EIP 1.5 devices

The following configuration is set on EIP 2.0+ devices but may not be set on EIP 1.5 devices and should be set manually in the admin interface of the device (CWIS):

- Job Accounting's User and Account Prompts
- Secure Access Setting of "Local login"
- Secure Access Setting of "Get accounting code from server"

8.1.3 Account selection and login without credit limitation for EIP 1.5 devices

By default, on an EIP 1.5 device it cannot force a user to select an account because it does not have the Job Limits feature to support this. Therefore, if you need to force the user to select an account on an EIP 1.5 device then you will need to set *ext-device.xerox.select-account* to "N" which will no longer use the Account Selection app to select an account. Instead, the user interface of the Secure Access login workflow will be used for the user to input an account.

Because, we cannot guarantee an account is selected, if the user has the ability to choose a shared account then we cannot know at login time whether they have enough balance or not. For example, the user may have \$0 in their personal account but there is \$20 in the Science account that they have access to. So at login time, when an account selection app is used, we cannot fairly stop the user from logging in. If you need to guarantee that a user cannot login without enough balance then you either need to set *ext-device.xerox.select-account* to "N" or change the account selection options so that the user cannot select a shared account.

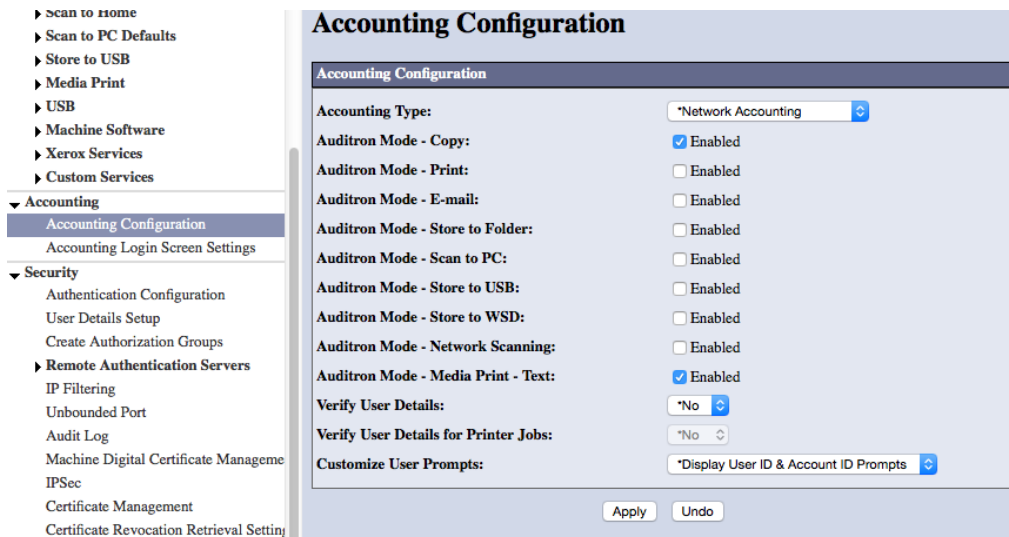
8.1.4 Login without credit and free scanning/faxing limitation on EIP 1.5 devices

Without the Job Limits feature, we have no way of knowing ahead of time what service the user is going to pick and we cannot stop them once they have logged in and are at the home screen. Therefore, to do a balance check we assume that the user is able to do a 1 page copy job and we will prevent the user logging in if they don't have enough balance to do so. This will then stop them even if they weren't going to do a copy job but instead were going to do a scan or fax job.

However, one option is to set up the MFP such that the Scanning service does not require any authentication and it can effectively bypass PaperCut. For example, on a Xerox 5325 (EIP 1.5), the following 2 settings can be done:

8.1.4.1 Disable the Job Accounting for scanning

1. Log in as the admin user.
2. Go to the Properties->Accounting->Accounting Configuration
3. Enable the Auditron Mode for the service that you want authentication on e.g. see attached screen shot which enables the Copy service but not the scanning services.



8.1.4.2 In Secure Access, turn off authentication for scanning

1. Login as the admin user
2. Go to Properties->Security->Authentication Configuration
3. Click Next
4. Click "Configure..." on Service Access

- Lock the services that you need authentication on and unlock the other services. For example, leave the scanning services unlocked.



8.1.5 Maximum of 30 concurrent fax jobs

Xerox EIP 1.5+ devices have a limitation of being able to hold a maximum of 30 concurrent fax jobs in the Active Jobs queue when Job Based Accounting is enabled on the device. Job Based Accounting is required by PaperCut

8.2 Faxing limitations summary

8.2.1 Fax Tracking

Many Xerox MFPs do not log sent faxes in the Network Accounting / JBA logs. On these devices PaperCut cannot track any outbound faxes.

Please check with Xerox whether your device model supports fax tracking via Network Accounting.

For example, the following Xerox devices do not support tracking faxes:

- ColorQube 8700
- ColorQube 8900
- WorkCentre 5735/5740/5745/5755
- WorkCentre 5765/5775/5790
- WorkCentre 7525/7530/7535/7545/7556

8.2.2 No Zero Stop for Faxing

Xerox devices currently do not stop fax jobs when users run out of credit. Instead, users can complete the fax job and possibly incur an overdraft in their accounts (if Fax Tracking is supported for that model).

8.3 User Interface limitations summary

The interface displayed during the user login process has some limitations. For EIP 1.5 devices, this is also used to select an account. The Xerox Secure Access features allow us to display any number of screens with either one of the following features:

1. A text input field (which can be optionally masked for password input)
2. A prompt with “Yes” and “No” buttons.

These limitations restrict the richness and flexibility that we can provide in the login process.

This is a limitation of the Xerox Secure Access system.

8.4 Bypassing the System limitations summary

It is important that the administrators take care to prevent users from bypassing the system and directly accessing the copier.

To ensure the system is secure, administrators should take the following precautions:

- The copier’s built in admin password should be changed from the default and always kept secure.
- The services should be locked down as specified in section 4.4.10.

8.5 Card Reader support for authentication limitations summary

PaperCut supports network card readers using common card formats. For more information, contact the PaperCut Authorized Solution Center in your region.

The Xerox Secure Access environment began supporting USB card readers in late 2011. Support for USB card readers is only available on some MFP devices with the latest firmware and Xerox is gradually rolling out support for USB card readers across their device range. Contact Xerox for information on what devices and firmware are required for USB card reader support.

8.6 EIP 2.0+ device limitations (Job Assembly not supported by default)

Xerox’s Job Assembly feature which allows one to program a job with different attributes such as different page sizes, is not supported if Job Limits is used. Job Limits is currently used by PaperCut for Zero Stop and potentially forcing Account Selection on EIP 2.0+ devices – it is not used on EIP 1.5 devices. If you require Job Assembly and do not require Zero Stop or enforcement of Account Selection, then you need PaperCut to disable the Job Limits’ preauthorizations on the Xerox MFP. Once this is done, the Job Assembly buttons will be enabled and the functionality should work.

If you do need to force the user to select an account then you can set *ext-device.xerox.select-account* to "N". Account Selection will then be done during the login workflow instead of by using the Account Selection App. Note that account selection done in this manner is not as user friendly.

8.6.1 Turning Off Job Limits’ Preauthorization

You need to do the following to disable the job limits from pre-authorizing jobs.

1. Log into PaperCut.

2. Navigate to the Xerox device’s details page.
3. Navigate to the Advanced Config and set `ext-device.xerox.enable-preauth` to “N” and click on the Update button. This configuration change will modify the Xerox device in a few seconds.

8.6.1.1 Check Preauthorization is disabled on Xerox MFP (optional)

Optionally, if you want to make sure that the previous configuration setting has happened, then you can check on the Xerox’s admin pages.

1. Login to the device’s web admin (CWIS).
2. Navigate to Properties > Login/Permissions/Accounting > Accounting Method.
3. Click on the Edit button for Accounting Workflow.



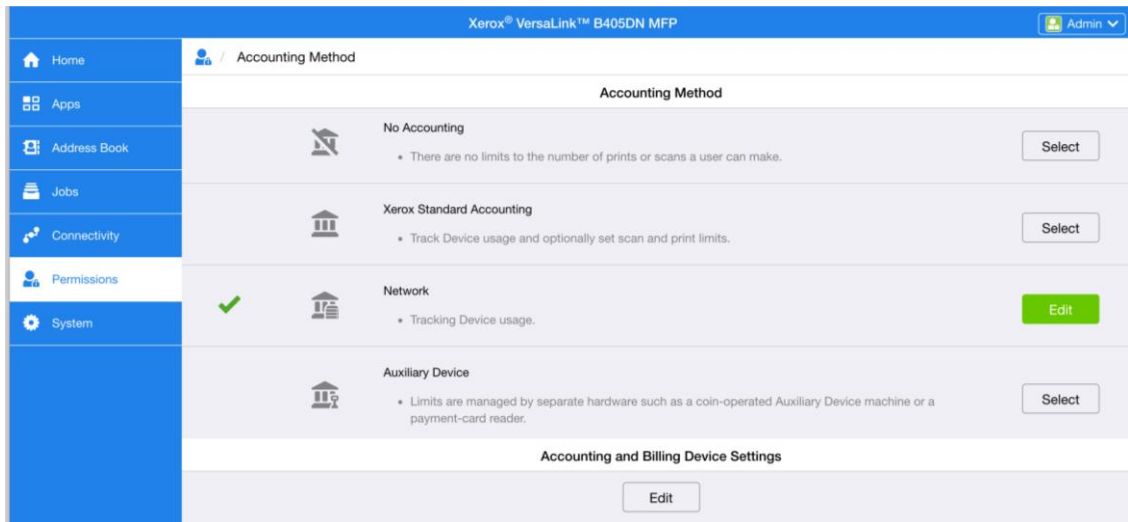
4. Verify that for all the job types that the Accounting Workflow is just set to “Capture Usage”.



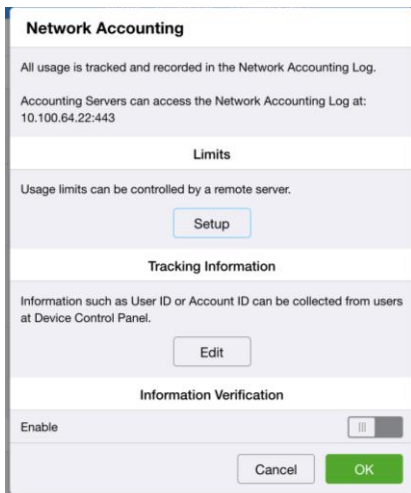
8.6.1.2 Check Preauthorization is disabled on VersaLink devices (optional)

If you want to make sure that the previous configuration setting has happened, then you can check on the Xerox’s admin pages.

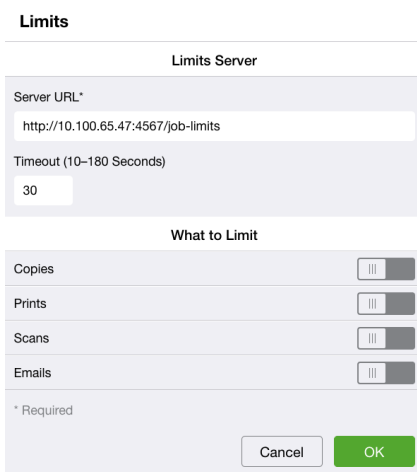
1. Login to the device's web admin (CWIS).
2. Navigate to Permissions > Accounting Method.
3. In the **Network Accounting Method**, click **Edit**.



4. In the **Limits Network Accounting** section, click **Setup**.



5. Verify that the **Copies, Prints, Scans, and Emails** toggles are set to **Off** (disabled).



6. Click 'OK'.

8.7 Unable to bypass authentication for custom Apps/Services

It is possible to decide whether a non-logged-in user is allowed to access a service or not. This can be set in the CWIS via Properties->Login/Permissions/Accounting->User Permissions->Services & Tools.

The screenshot shows the 'Properties' window in the PaperCut configuration tool, specifically the 'User Permissions' section. The 'Presets' area at the top has four radio buttons: 'Allow access to everything except Tools (Standard Access)', 'Allow access to everything including Tools (Open Access)', 'Restrict access to all Services and Tools', and 'Restrict access to everything'. The 'Custom' option is selected. Below this is a table with two columns: 'Name' and 'Role State'. The table lists various services and their current access states.

Name	Role State
Machine Status Pathway	Allowed
Tools (Touch & Web UI)	Allowed
Job Status Pathway	Allowed
Job Deletion (Active Queue Only)	Allowed
Services Pathway	Not Allowed
Copy	Not Allowed & Hidden
Color Copy	Not Allowed
ID Card Copy	Not Allowed & Hidden
Color Copy	Not Allowed
Email	Not Allowed & Hidden
Scan To...	Not Allowed & Hidden
Workflow Scanning	Not Allowed & Hidden
Print From	Not Allowed & Hidden
PaperCut Account Selection	Not Allowed & Hidden
PaperCut Print Release	Not Allowed & Hidden

At the bottom of the window are 'Close' and 'Apply' buttons.

Potentially, it can allow one to access a service without requiring authentication which may be useful in some circumstances. An example, might be allowing Xerox's Mobile Print App to be selected without requiring initial authentication. However, if one "allows" an additional App to be used without logging in, then it will pop up an Accounting dialog which requests a User ID and an Account which makes no sense to the user and we do not want. This is triggered by having the User Accounting Prompts enabled for services.

User Accounting Prompts

Prompt	Display Prompt	Label	Default Value	Mask Entries (***)
1	<input checked="" type="radio"/> Yes <input type="radio"/> No	User ID abc		<input type="radio"/> Yes <input checked="" type="radio"/> No
2	<input checked="" type="radio"/> Yes <input type="radio"/> No	Account ID		<input type="radio"/> Yes <input checked="" type="radio"/> No

Services

Services	No Prompt	Prompt	Color Prompt Only
Copies ¹	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Prints	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Scans	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Email ¹	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Workflow Scanning ¹	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Note

1) Prompts are always required for the following services when [Accounting Workflow is Pre-Authorization and Capture Usage](#).
 Copy
 Email
 Workflow Scanning

When 'No Prompts' option is configured for other services, then generic codes will be used if accounting codes do not exist in jobs.

The User Accounting Prompts are needed for Xerox's Job Limits feature which allows PaperCut to do Zero Stop and tracking of Shared Accounts. The prompts are also used for tracking usernames in the job log. Therefore, the User Accounting Prompts are essential to PaperCut's solution for Xerox which means we are unable to support the custom Apps without them being set to require authentication.

8.8 Integrated Scanning limitations summary

- Since devices without an automatic document feeder (ADF) still have duplex as an available option in the **Scan Setting** page on the device, all duplex scan jobs default to simplex jobs.
- Depending on the device, scanning to TIFF may result in an older TIFF formatted file.
- When scanning to TIFF, a separate file is sent for each scanned page.
- When a user fails to place an actual document to scan on the platen or the feeder, this is not detected and scanning continues without prompting the user to place actual documents to scan.
- An Integrated Scanning scan job that is in progress is cancelled, if the user attempts to log out using the device hard key while the scan job is in progress.
- Cancelling an Integrated Scan job on VersaLink devices still tracks the scan job as completed.

9 How it works

The following section gives a brief overview of the internal workings of PaperCut's on-board solution for Xerox devices. It's provided as background information and may be useful for technical administrators in troubleshooting problems.

Typical function workflow:

1. A user logs into the MFP via the panel. The MFP is configured to contact PaperCut (via SOAP web services) to verify login information.
2. The user ID and password is validated and device access is granted as appropriate.
3. If "release jobs on login" is enabled, any waiting jobs are immediately queued for printing. (called secure print release or find-me printing)
4. If the user performs any device functions such as Copy, Fax or Scan, these are recorded against the user ID in the device's onboard logs.
5. On EIP 2.0+ devices, if PaperCut is tracking a device function, then at the start of the job it will send a SOAP message to PaperCut asking authorization to print the job or not. PaperCut will look at the attributes of the job and decide if the charging account has enough money to pay for the job. If it does then the job will proceed, otherwise an error message will be displayed. This is how the Zero Stop functionality works.
6. At regular periods (e.g. every minute) PaperCut contacts the device looking for new log entries (logs are downloaded via HTTP using JBA network accounting).
7. Any new log entries are analyzed and recorded in PaperCut's usage database. Any cost associated with the usage is charged from the user's account (or their selected Shared Account).

10 FAQ & Troubleshooting

PaperCut shows an error status for the device. What could cause this?

In the “Devices” list the Xerox device may appear with an error status (hover your mouse over the status to see the full status message). The status message will help understand the cause of the error. The most common cause of problems is due to a networking issue, to resolve:

- Verify that the device network address (or IP) is entered correctly in PaperCut
- Verify that networking and firewalls allow PaperCut to establish a connection to the device on TCP ports 80 and 443 and UDP port 161 for SNMP.
- Verify that the SNMP configuration enabled in the device’s web interface aligns with the configuration in PaperCut MF. For more information, see [4.4.4 SNMP version](#).
- Verify that networking and firewall settings allow the device to establish connections to the PaperCut server on ports 9191 and 9192.
- Verify that you have provided the correct administrator login credentials for the device in the PaperCut device configuration page.

Another common cause of errors is that “Network Accounting / JBA” has not been enabled/configured on the device. Ensure that the Network Accounting is enabled as described in section 4.4.7.

Another possible cause of problems is if the device firmware does not support the “Off-box validation” features required by PaperCut. This feature should be available for recent Xerox copiers supporting “Network Accounting”, however sometimes a firmware upgrade is required.

How often does PaperCut poll for accounts?

Account validation is done in real-time using the Xerox authentication web services methods. Hence any changes made to Shared Accounts, user rights, or user passwords are available immediately.

How often does PaperCut poll for job activity?

Within 10 minutes of device login, job activity is checked either:

- at the interval defined by `ext-device.xerox.job-download-after-login-period-secs`
- if no interval is defined:
 - every 10 seconds without job-limits
 - every 30 seconds with job-limits

During idle time, job activity is checked either:

- at the interval defined by `ext-device.xerox.job-download-period-mins`
- if no interval is defined, every 5 minutes

Can I use a hostname rather than an IP address in the URLs when configuring the release station settings?

Using a hostname relies on the MFD using your DNS and ensuring that your DNS is correctly configured. The quickest failsafe option is to use the server’s IP. If you have advanced networking skills, you may wish to investigate using a hostname.

The device displays an error when authenticating the user.

The most likely cause of problems is that the device cannot establish a connection to the PaperCut server. Make sure that your networking/firewalls allow network connections from the device to the PaperCut server on ports 9191 and 9192.

Also ensure that the device SSL/HTTPS options are enabled. Ensure that the option to “Verify the remote server certificate” is disabled.

If your PaperCut server has multiple IP addresses or you use NAT on your network, see section 7.2 on how to explicitly configure the PaperCut server’s network address.

On some EIP 1.5 devices (such as WorkCentre 5325), the device may need to be rebooted for it to properly register the Secure Access URL to use.

The device status displays:

Error: Xerox HTTP error calling: https://192.168.2.101/acct/get_config - Response: 404 (Not found)

This error can be due to a failure to configure the Xerox Network Accounting on the device.

- If you have a VersaLink device, restart your device (Home -> Support -> Restart Device).
- If you have other devices, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.

I see an error on the Xerox LCD screen?

This may indicate networking issue, a configuration issue, or maybe a software bug. Re-check your settings and restart the MFD (i.e. power off and power on the copier). If problems continue, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut Admin interface on the **About** page.

The PaperCut device status displays the following error:**Error: User authentication failed IPLockedOut: Excessive Failure Attempts**

This error can occur if you have the incorrect username and password set up for the PaperCut device. Even if you then set the correct username and password you can be locked out for a while. To reset the lockout, you can go to the following page:

<http://device-address/diagnostics/ipLockout.php>

The “Build Job” and “Sample Job” buttons are greyed out. What is wrong?

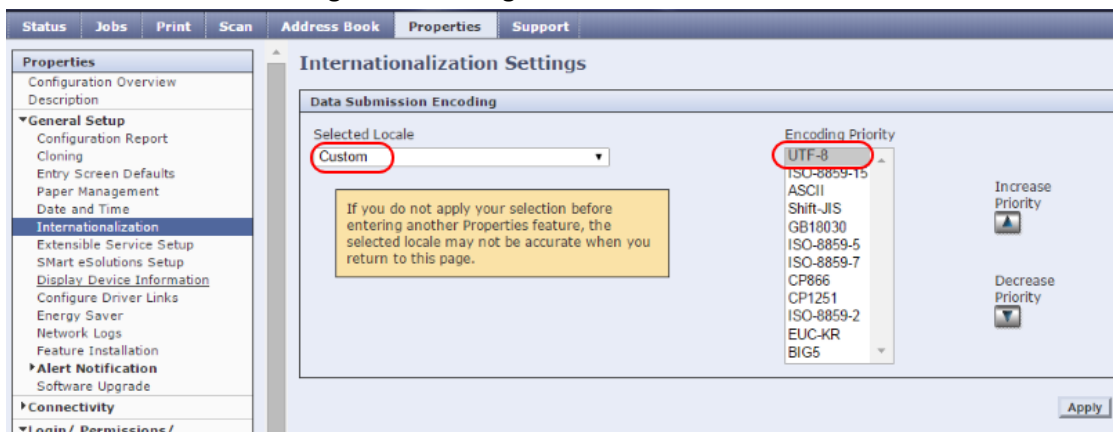
This should only be an issue on EIP 2.0+ devices and not on EIP 1.5 devices. The Job Assembly feature of the Xerox, unfortunately, is not compatible with Job Limits and therefore the Job Assembly buttons are disabled by default. If you need this functionality and don’t need Zero Stop, then see section 8.6.

Some accented characters do not appear correctly on the MFP panel on some devices. How can we display these characters?

On some Xerox devices, such as the WC 75xx models, we have seen issues with accented characters such as French and Norwegian.

Change the settings below on the device's web page (CWIS):

1. Properties → General Setup → Internationalization → Selected Locale = Custom
2. Properties → General Setup → Internationalization → Encoding Priority for "UTF-8" to be 1st Priority
3. Reboot the MFP after changed that setting



Can the device panel buttons be used for Integrated Scanning?

The device panel buttons can be used for the following:

- When on the **Scan Details** screen or the **Scan Settings** screen, the **Start** button can be used to start a new scan job.
- When on the **Scan More or Finish** screen, the **Start** button can be used to complete (finish and send) the current job and start a new scan job.
- When on the **Scan In Progress** screen, the **Stop** button can be used to cancel a scan job that is in progress.