PaperCut MF - Xerox Secure Access EIP1.5+ Embedded Manual

Contents

1 Document revision history

Published date or release	Details of changes made
21.2	5.9 Phonebook contacts
20.0.4	2.8 Setup procedure for AltaLink C8100 series & EC8000 series devices
20 December 2019	Document restructure
19.2.0	4.3.6 Install PaperCut MF; 6.5 Secure Print Release; 6.8.2 Header logo; 6.9 Config Editor
19.0.3	8.1.3 Account selection and login without credit limitation for EIP 1.5 devices
19.0.0	2 Overview; 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; 6.2 Held print job settings at the device; 7.1 Config Editor
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 Installation

This section covers the installation of *PaperCut MF - Xerox (Secure Access EIP 1.5+)*

2.1 Supported devices

Ensure that the devices on the network are listed as supported devices on the PaperCut MF for Xerox page.

2.2 Compatible devices

Ensure that supported Xerox devices on the network are compatible with PaperCut's embedded software solution *PaperCut MF - Xerox (Secure Access EIP 1.5+):*

- they have a hard disk installed and configured
- they are covered by Xerox's **Network Accounting Kit** / **JBA Accounting** license; "End of Life" devices are unsupported and incompatible
- they are running the Xerox Secure Access Extensible Interface Platform (EIP) version 1.5 or above:
    - **Discovery (Legacy)**
        - Running EIP 1.5, such as:
          5735, 5745, 5755, 5765, 7525, 7530, 7535, 7545, 7556, 77xx, with SPAR Release Firmware 061.121.229.02600(R19-01)
        - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA), tracking, charging and logging of most device jobs*, *etc*
    - **EIP/JBA Fuji-Xerox devices**
        - Running EIP 1.5, such as:
          5325, 5330, 5335, with SPAR Release Firmware 53.34.23
          5220, 5225, 7120, 7125, 73xx, C550, C560, C60, C70, D95, D110, D125, D136
        - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA), tracking, charging and logging of most device jobs*, *etc*
    - **ConnectKey 1.0 devices**
        - ConnectKey 1.0 devices running EIP 2.0, such as:
          ColorQube 8700, 8900, 9301, 9302, 9303, with SPAR Release Firmware 072.xxx.009.07200
        - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA), tracking, charging, logging and controlling (Zero Stop) of most device jobs*, *etc*
    - **ConnectKey 2.5 devices**
        - ConnectKey 2.5 devices running EIP 3.0, such as:
          3635, 58xx, 59xx, 6655, 7220, 7225, 7835, 7845, 7970, with SPAR Release Firmware 073.xxx.059.25300 (R19-08); 073.xxx.019.13010(R19-05)
        - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA),*

tracking, charging, logging and controlling (Zero Stop) of device jobs, Integrated Scanning, customization of device screens, changing attributes (account, pages, color) of held print jobs, etc

- **VersaLink devices**
    - Running EIP 3.7, such as:
      multi-function devices C405, C505, B405, B605, B7035, B7030, with SPAR Release Firmware xx.52.01 PL6-R1
      single function devices C400, C500, C600, C7000, C8000, C9000, B400, B600, B610, with SPAR Release Firmware xx.52.01 PL6-R1
    - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA), tracking, charging, logging and controlling (Zero Stop) of device jobs, Integrated Scanning, customization of device screens, changing attributes (account, pages, color) of held print jobs, etc*
- **AltaLink devices**
    - Running EIP 4.0, such as:
      C8070, C8045, C8055, C8030, C8035, C7045, B8030, B8035, B8045, B8090, with SPAR Release Firmware 101.xxx.099.28200 (R19-09)
    - PaperCut MF features include: *User authentication, secure print release, tracking and charging of held print jobs, secure access to device jobs (XSA), tracking, charging, logging and controlling (Zero Stop) of device jobs, Integrated Scanning, customization of device screens, changing attributes (account, pages, color) of held print jobs, etc*

Note: This manual is only relevant to supported and compatible Xerox devices. For more information on PaperCut's embedded software solutions for other devices and platforms, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut MF Admin web interface, on the **About** page.

2.2.1 Important information for Xerox 3rd Generation Browser compatibility

For Xerox devices with 3rd Generation Browsers only (devices such as VersaLink B625 and Altalink 8100 series with Service Pack R23-02), please ensure your device PaperCut MF version is updated to PaperCut MF 22.0.9 or later.

2.3 System requirements

Ensure that the following system requirements are met:

- The following entities are available:
    - Physical device – administrator and user access, and credentials
    - Device's web interface (CWIS) – administrator access, URL, and credentials
    - PaperCut MF Admin web interface – administrator access, URL, and credentials
- The latest version of the PaperCut MF Application Server is installed and running on the network. For more information, see the PaperCut MF manual.
  Note: The minimum compatible version is 18.0.2 or above.
- The networking/firewall configuration allows:

- Inbound connections to the PaperCut MF Application Server from the devices on the configured ports. For example:
    - 9191 (TCP/HTTP)
    - 9192 (SSL/TLS/HTTPS)
- Outbound connections from the PaperCut MF Application Server to the devices on the configured ports. For example:
    - 80 (TCP/HTTP)
    - 443 (SSL/TLS/HTTPS)

2.4 Setup procedure for EIP/JBA Fuji-Xerox devices (EIP 1.5)

To set up PaperCut MF on EIP/JBA Fuji-Xerox devices (running EIP 1.5), you must:

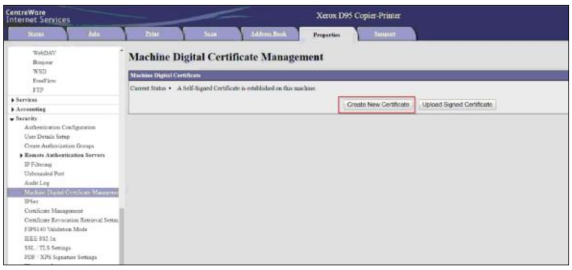
- 2.4.1 Configure the device’s security settings
- 2.4.2 Configure the device’s SNMP settings
- 2.4.3 Configure the device’s EIP settings
- 2.4.4 Configure the device’s accounting settings
- 2.4.5 Install PaperCut MF
- 2.4.6 Configure the device’s XSA authentication settings
- 2.4.7 Configure the device’s user access permission settings

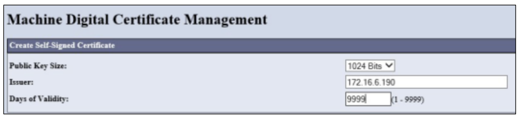
Note: The navigation, instructions and images of the device and the device’s web interface are of EIP/JBA Fuji-Xerox devices, running EIP 1.5, 5325 and D95. This could vary on other EIP 1.5 devices.

2.4.1 Configure the device’s security settings

To configure the device’s security settings:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > Security > Machine Digital Certificate Management**.
3. Click **Create New Certificate**.
4. Enter the required details:

5325	D95
	 Machine Digital Certificate Management Current Status • A Self-Signed Certificate is established on this machine



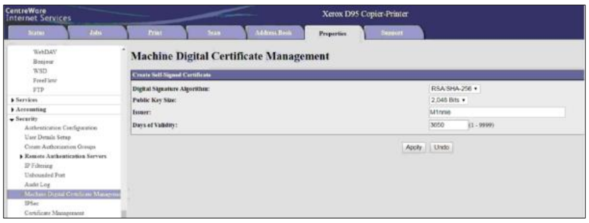
Machine Digital Certificate Management

Create Self-Signed Certificate

Public Key Size: 1024 Bits

Issuer: 172.16.6.190

Days of Validity: 9999 (1 - 9999)



Machine Digital Certificate Management

Create Self-Signed Certificate

Digital Signature Algorithm: RSA/SHA-256

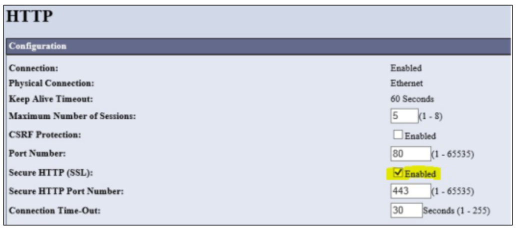
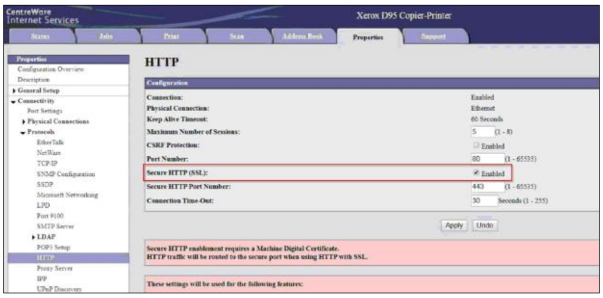
Public Key Size: 2,048 Bits

Issuer: [illegible]

Days of Validity: 3650 (1 - 9999)

5. Click **Apply**.
6. Restart the device.
7. Navigate to **Properties > Services > Printing > Printing Web Services.**
8. In **Authentication & Accounting**, ensure **Xerox Secure Access** is NOT selected.
9. Navigate to **Properties > Security > Remote Authentication Servers > Xerox Secure Access**.
10. In **Local Login**, ensure **Xerox Secure Access** is NOT selected.

    Note: This is because, the HTTPS protocol cannot be changed if Xerox Secure Access is enabled. So, you must first disable Xerox Secure Access before attempting to enable HTTPS.
11. Restart the device.
12. Navigate to **Properties > Connectivity > Protocols > HTTP.**
13. In **Secure HTTP (SSL)**, select **Enabled.**

5325	D95
	

HTTP

Configuration

Connection: Enabled

Physical Connection: Ethernet

Keep Alive Timeout: 60 Seconds

Maximum Number of Sessions: 5 (1 - 8)

CSRF Protection: ☐ Enabled

Port Number: 80 (1 - 65535)

Secure HTTP (SSL): ☑ Enabled

Secure HTTP Port Number: 443 (1 - 65535)

Connection Time-Out: 30 Seconds (1 - 255)

HTTP

Configuration

Connection: Enabled

Physical Connection: Ethernet

Keep Alive Timeout: 60 Seconds

Maximum Number of Sessions: 5 (1 - 8)

CSRF Protection: ☐ Enabled

Port Number: 80 (1 - 65535)

Secure HTTP (SSL): ☑ Enabled

Secure HTTP Port Number: 443 (1 - 65535)

Connection Time-Out: 30 Seconds (1 - 255)

Secure HTTP enablement requires a Machine Digital Certificate.
HTTP traffic will be routed to the secure port when using HTTP with SSL.

These settings will be used for the following features:

14. Click **Apply.**
15. Restart the device.

2.4.2 Configure the device’s SNMP settings

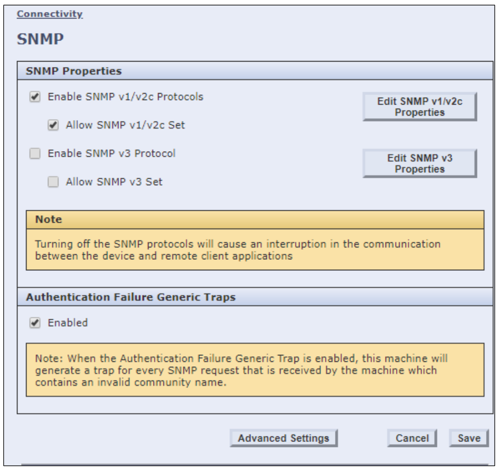
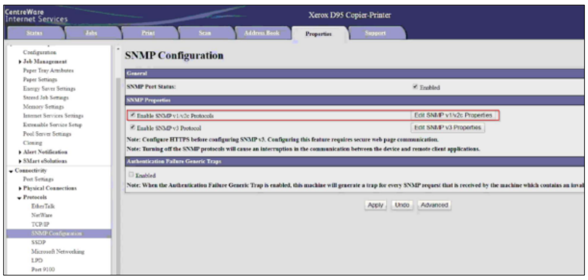
You can configure the device to use any one of the following SNMP settings:

- 2.4.2.1 SNMPv1/v2c
- 2.4.2.2 SNMPv3

2.4.2.1 SNMPv1/v2c

To configure the device to use SNMPv1/v2c:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > Connectivity > Protocols > SNMP Configuration.**
3. Select **Enable SNMP v1/v2c Protocols** and **Allow SNMP v1/v2c Set**:

5325	D95
	

SNMP

SNMP Properties

☑ Enable SNMP v1/v2c Protocols

☑ Allow SNMP v1/v2c Set

☐ Enable SNMP v3 Protocol

☐ Allow SNMP v3 Set

Note

Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications

Authentication Failure Generic Traps

☑ Enabled

Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

SNMP Configuration

General

SNMP Port Status: ☑ Enabled

SNMP Properties

☑ Enable SNMP v1/v2c Protocols

☑ Enable SNMP v3 Protocol

Note: Configure HTTPS before configuring SNMP v3. Configuring this feature requires secure web page communication.

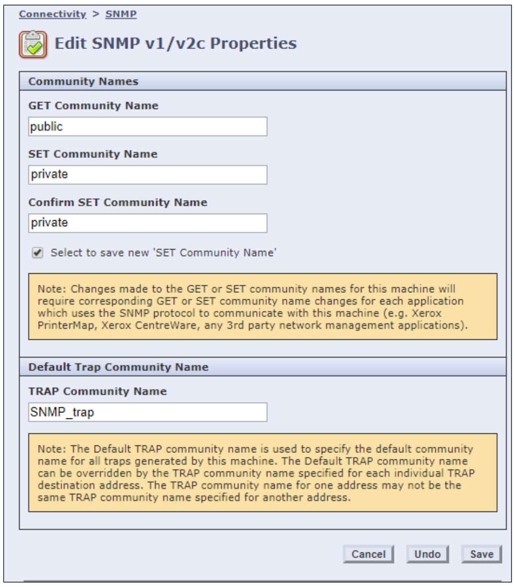
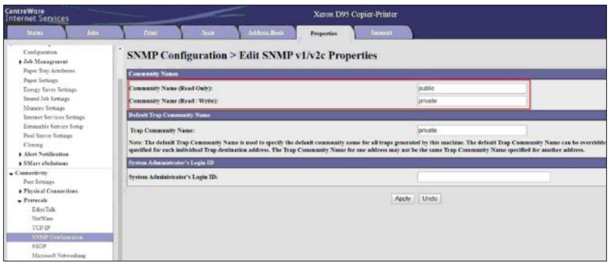
Note: Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications.

Authentication Failure Generic Traps

☐ Enabled

Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an

4. Click **Edit SNMP v1/v2c Properties**.
5. In all the **Community Name** fields, enter relevant values:

5325	D95
	

Edit SNMP v1/v2c Properties

Community Names

GET Community Name: public

SET Community Name: private

Confirm SET Community Name: private

☑ Select to save new 'SET Community Name'

Note: Changes made to the GET or SET community names for this machine will require corresponding GET or SET community name changes for each application which uses the SNMP protocol to communicate with this machine (e.g. Xerox PrinterMap, Xerox CentreWare, any 3rd party network management applications).

Default Trap Community Name

TRAP Community Name: SNMP_trap

Note: The Default TRAP community name is used to specify the default community name for all traps generated by this machine. The Default TRAP community name can be overridden by the TRAP community name specified for each individual TRAP destination address. The TRAP community name for one address may not be the same TRAP community name specified for another address.

SNMP Configuration > Edit SNMP v1/v2c Properties

Community Names

Community Name (Read Only): public

Community Name (Read / Write): private

Default Trap Community Name

Trap Community Name: private

Note: The default Trap Community Name is used to specify the default community name for all traps generated by this machine. The default Trap Community Name can be overridde specified for each individual Trap destination address. The Trap Community Name for one address may not be the same Trap Community Name specified for another address.

System Administrator's Login ID

System Administrator's Login ID:

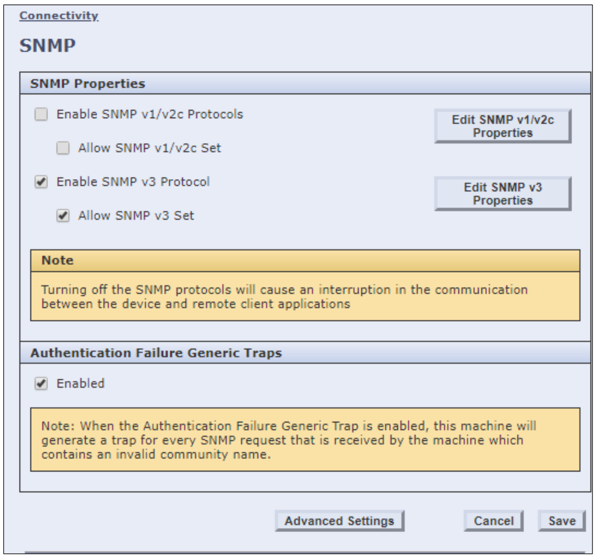
6. Take note of the **SET Community Name/ Community Name (Read/Write).**
7. Click **Save.**
8. Restart the device.

2.4.2.2 SNMPv3

To configure the device to use SNMPv3:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Connectivity > Protocols > SNMP Configuration.**

3. Select **Enable SNMP v3 Protocol** and **Allow SNMP v3 Set**:



☐ Enable SNMP v1/v2c Protocols
☐ Allow SNMP v1/v2c Set
☑ Enable SNMP v3 Protocol
☑ Allow SNMP v3 Set

Note

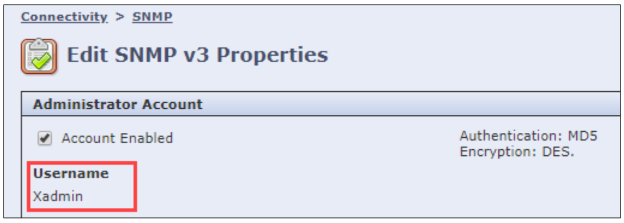
Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications

Authentication Failure Generic Traps

☑ Enabled

Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

4. Click **Edit SNMP v3 Properties**.
5. In **Administrator Account**, select **Account Enabled**.
6. Take note of the **SNMP v3 Authentication Username/ Security Name:**

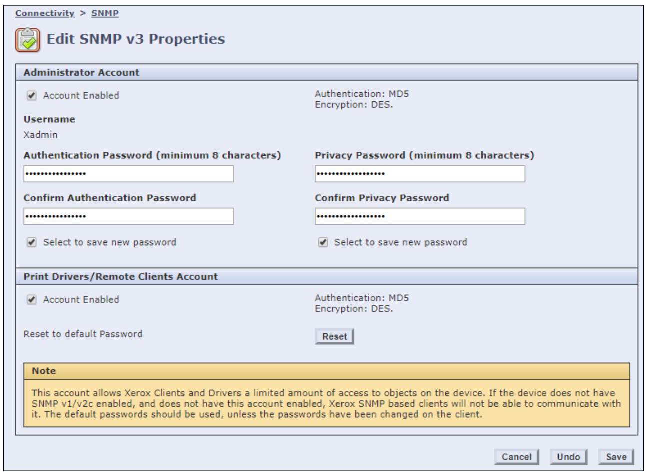


☑ Account Enabled

Authentication: MD5
Encryption: DES.

Username
Xadmin

7. In **Authentication Password** and **Privacy Password / Encryption Password**, enter relevant values:



Administrator Account

☑ Account Enabled

Authentication: MD5
Encryption: DES.

Username
Xadmin

Authentication Password (minimum 8 characters)

Privacy Password (minimum 8 characters)

Confirm Authentication Password

Confirm Privacy Password

☑ Select to save new password
☑ Select to save new password

Print Drivers/Remote Clients Account

☑ Account Enabled

Authentication: MD5
Encryption: DES.

Reset to default Password

Note

This account allows Xerox Clients and Drivers a limited amount of access to objects on the device. If the device does not have SNMP v1/v2c enabled, and does not have this account enabled, Xerox SNMP based clients will not be able to communicate with it. The default passwords should be used, unless the passwords have been changed on the client.

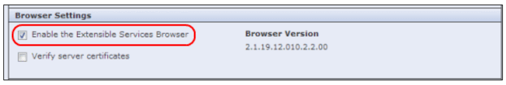
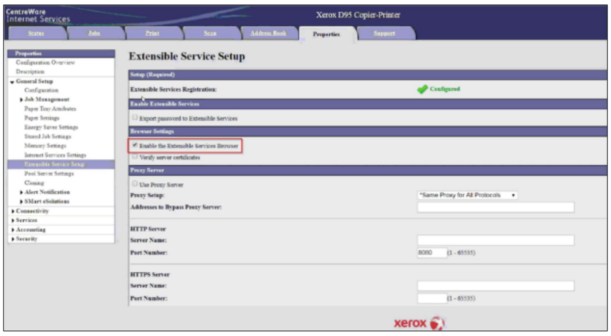
8. Take note of the **Authentication Password** and the **Privacy Password / Encryption Password**.
9. Click **Save.**
10. Restart the device.

2.4.3 Configure the device’s EIP settings

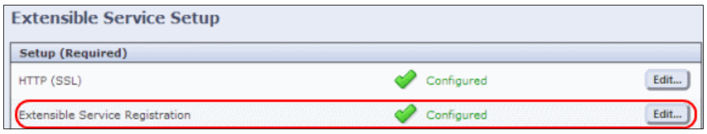
To configure the device’s EIP settings:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > General Setup > Extensible Service Setup.**

3. In **Browser Settings**, select **Enable the Extensible Services Browser**.

5325	D95
 **Browser Settings** ☑ Enable the Extensible Services Browser ☐ Verify server certificates **Browser Version** 2.1.19.12.010.2.2.00	 CentreWare Internet Services Xerox D95 Copier-Printer Extensible Service Setup **Setup (Required)** Extensible Services Registration: Configured **Enable Extensible Services** ☐ Export password to Extensible Services **Browser Settings** ☑ Enable the Extensible Services Browser ☐ Verify server certificates **Proxy Server** ☐ Use Proxy Server Proxy Setup: *Same Proxy for All Protocols Addresses to Bypass Proxy Server: **HTTP Server** Server Name: Port Number: 8080 (1 - 65535) **HTTPS Server** Server Name: Port Number: (1 - 65535)

4. In **Setup > Extensible Service Registration**, click **Edit**.

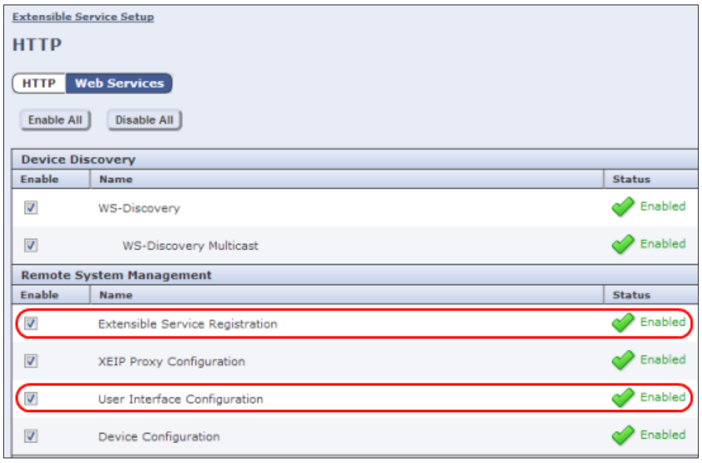


Extensible Service Setup

Setup (Required)

HTTP (SSL)	Configured	Edit...
Extensible Service Registration	Configured	Edit...

5. In **Remote System Management**, select **Extensible Service Registration** and **User Interface Configuration**.



Extensible Service Setup

HTTP

Device Discovery

Enable	Name	Status
☑	WS-Discovery	Enabled
☑	WS-Discovery Multicast	Enabled

Remote System Management

Enable	Name	Status
☑	Extensible Service Registration	Enabled
☑	XEIP Proxy Configuration	Enabled
☑	User Interface Configuration	Enabled
☑	Device Configuration	Enabled

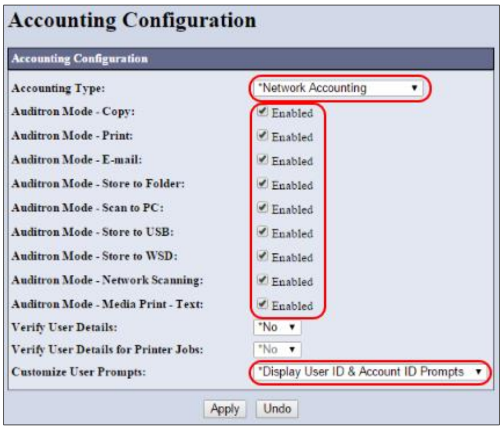
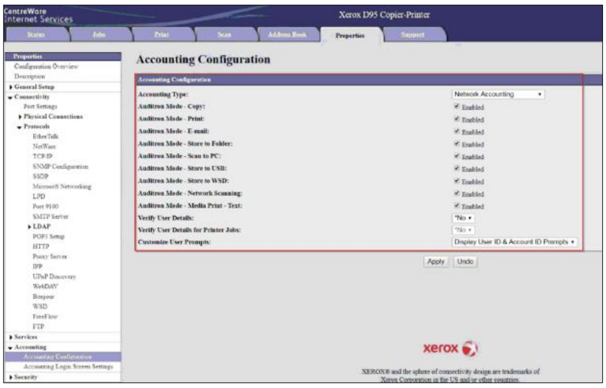
6. Click **Apply**.
7. Restart the device.

2.4.4 Configure the device's accounting settings

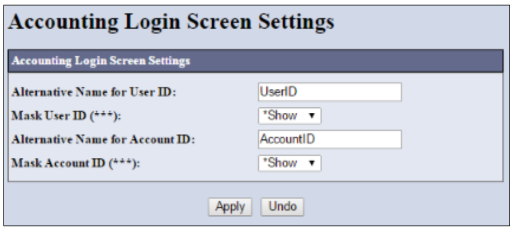
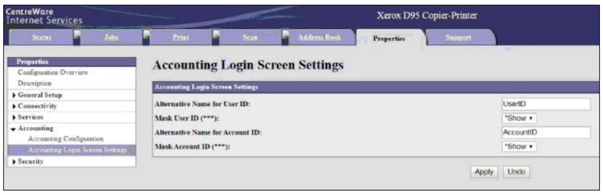
Note: This is only applicable to multi-function devices.

To configure the device's accounting settings to ensure that jobs are accurately logged:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Accounting > Accounting Configuration**.
3. In **Accounting Type**, select **Network Accounting**.
4. For all **Auditron Modes**, select **Enabled**.
5. In **Customize User Prompts**, select **Display User ID & Account ID Prompts**.

5325	D95
 Accounting Configuration Accounting Type: *Network Accounting Auditron Mode - Copy: ☑ Enabled Auditron Mode - Print: ☑ Enabled Auditron Mode - E-mail: ☑ Enabled Auditron Mode - Store to Folder: ☑ Enabled Auditron Mode - Scan to PC: ☑ Enabled Auditron Mode - Store to USB: ☑ Enabled Auditron Mode - Store to WSD: ☑ Enabled Auditron Mode - Network Scanning: ☑ Enabled Auditron Mode - Media Print - Text: ☑ Enabled Verify User Details: *No Verify User Details for Printer Jobs: *No Customize User Prompts: *Display User ID & Account ID Prompts	 Accounting Configuration Accounting Type: Network Accounting Auditron Mode - Copy: ☑ Enabled Auditron Mode - Print: ☑ Enabled Auditron Mode - E-mail: ☑ Enabled Auditron Mode - Store to Folder: ☑ Enabled Auditron Mode - Scan to PC: ☑ Enabled Auditron Mode - Store to USB: ☑ Enabled Auditron Mode - Store to WSD: ☑ Enabled Auditron Mode - Network Scanning: ☑ Enabled Auditron Mode - Media Print - Text: ☑ Enabled Verify User Details: *No Verify User Details for Printer Jobs: *No Customize User Prompts: Display User ID & Account ID Prompts

6. Click **Apply**.
7. Restart the device.
8. Navigate to **Properties > Accounting > Accounting Login Screen Settings**.
9. In **Alternative Name for the User ID**, select **UserID**.
10. In **Alternative Name for the Account ID**, select **AccountID**.

5325	D95
 Accounting Login Screen Settings Alternative Name for User ID: UserID Mask User ID (***): *Show Alternative Name for Account ID: AccountID Mask Account ID (***): *Show	 Accounting Login Screen Settings Alternative Name for User ID: UserID Mask User ID (***): *Show Alternative Name for Account ID: AccountID Mask Account ID (***): *Show

11. Click **Apply**.
12. Restart the device.

2.4.5 Install PaperCut MF

To install PaperCut MF (i.e. device registration and integration):

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

2.4.5.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 introduced a feature to create multiple devices in bulk through a CSV file via server commands. In 20.0.0 we added a way to load this CSV file via the PaperCut MF UI. You can find the feature under: PaperCut MF > Devices > Create multiple devices.

Using this feature increases your operational efficiency by significantly reducing the time taken to add devices to PaperCut MF. From version 20.0, this feature also allows for you to add devices to PaperCut MF before such devices are delivered to their installation site, such devices are added with a “Staged” status. The scenario for “Staged” devices applies when the system admin already knows all the device’s attributes prior to its delivery. For more information, see the Enhanced Deployment Project.

2.4.5.2 Install PaperCut MF on each device

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

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**
4. In **Type**, select the applicable option, depending the device:
   - for multi-function devices, select **Xerox (Secure Access EIP 1.5+)**
   - for single function devices, select **Xerox (Secure Access EIP 1.5+) Print Only**
5. In **Device name**, enter a descriptive name for the device.
6. Optionally, in **Location/Department**, enter location or department details of the device.
7. In **Hostname / IP**, enter the network name or IP address of the device.
8. In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device’s web interface.
9. To enable PaperCut MF to use:
   - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox is not selected (default).
   - SNMPv3, select the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox; and enter the following fields:
     - **Context name** – Do not enter any value.
     - **Username** – Enter **Xadmin**.
     - **Privacy password** – Enter the same value as the device web interface’s **Privacy/ Encryption Password.**
     - **Authentication password** – Enter the same value as the device web interface’s **Authentication Password.**
     - **Authentication protocol** – Select **MD5.**
     - **Privacy protocol** – Select **DES.**

   Note: For more information, see 4.5 SNMP.
10. In **Function**, select the required device jobs:
    - **Track & control copying**
    - **Track & control scanning**

   - **Track & control faxing**
   - **Enable print release**

   Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.

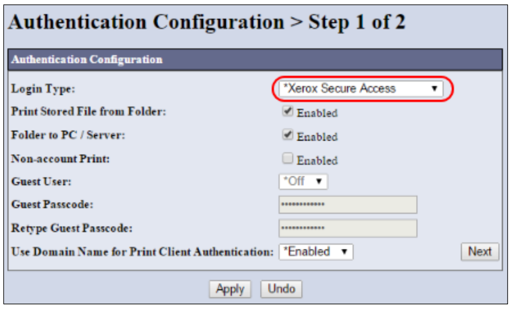
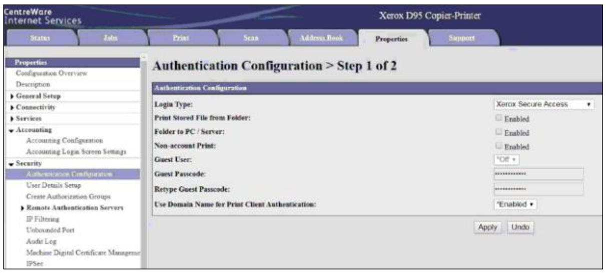
11. Click **Ok**.
12. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):
    - The PaperCut MF Admin web interface's **Device Status** displays the status **Started - Device is ready for user to login**.

2.4.6 Configure the device's XSA authentication settings

Note: This is only applicable to multi-function devices.

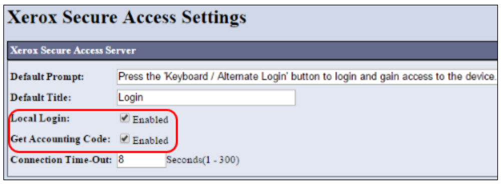
To configure the device's XSA authentication settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Services > Printing > Printing Web Services.**
3. In **Authentication & Accounting**, enable **Xerox Secure Access**.
4. Click **Apply**.
5. Restart the device.
6. Navigate to **Properties > Security > Authentication Configuration**.
7. In **Login Type**, select **Xerox Secure Access**.

5325	D95
 Authentication Configuration > Step 1 of 2 Login Type: *Xerox Secure Access Print Stored File from Folder: ☑ Enabled Folder to PC / Server: ☑ Enabled Non-account Print: ☐ Enabled Guest User: *Off Guest Passcode: ••••••••••••• Retype Guest Passcode: ••••••••••••• Use Domain Name for Print Client Authentication: *Enabled	 Authentication Configuration > Step 1 of 2 Login Type: Xerox Secure Access Print Stored File from Folder: ☐ Enabled Folder to PC / Server: ☐ Enabled Non-account Print: ☐ Enabled Guest User: *Off Guest Passcode: ••••••••••••• Retype Guest Passcode: ••••••••••••• Use Domain Name for Print Client Authentication: *Enabled

8. Click **Apply.**
9. Restart the device.
10. Navigate to **Properties > Security > Remote Authentication Servers >** Authentication System.
11. In Authentication System, select Authentication Agent.
12. Click **Apply.**
13. Restart the device.
14. Navigate to **Properties > Security > Remote Authentication Servers > Xerox Secure Access Settings**.
15. In **Local Login**, select **Enabled**.
16. In **Get Accounting Code**, select **Enabled**.

5325	D95



Xerox Secure Access Settings

Xerox Secure Access Server

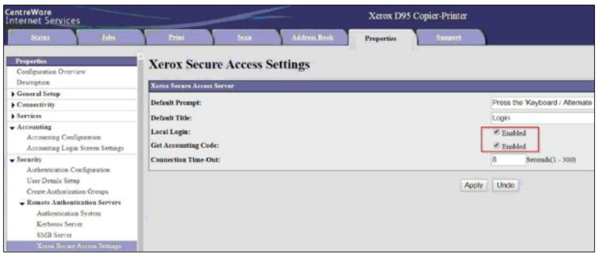
Default Prompt: Press the 'Keyboard / Alternate Login' button to login and gain access to the device.

Default Title: Login

Local Login: ☑ Enabled

Get Accounting Code: ☑ Enabled

Connection Time-Out: 8 Seconds(1 - 300)



Xerox Secure Access Settings

Xerox Secure Access Server

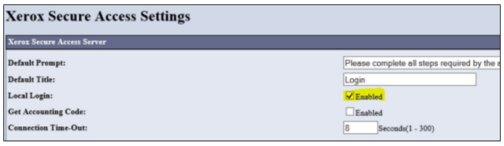
Default Prompt: Press the 'Keyboard / Alternate

Default Title: Login

Local Login: ☑ Enabled

Get Accounting Code: ☑ Enabled

Connection Time-Out: 8 Seconds(1 - 300)



Xerox Secure Access Settings

Xerox Secure Access Server

Default Prompt: Please complete all steps required by the

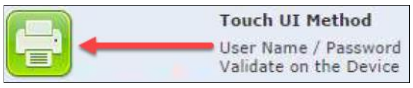
Default Title: Login

Local Login: ☑ Enabled

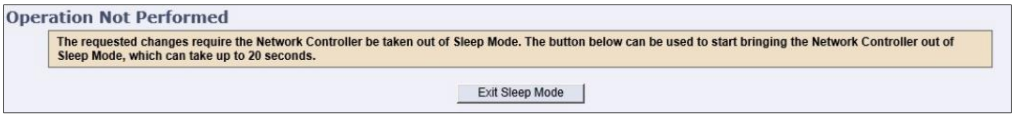
Get Accounting Code: ☐ Enabled

Connection Time-Out: 8 Seconds(1 - 300)

17. Click **Apply.**
18. Restart the device.
19. Navigate to
20. Click the **Touch UI Method** button (top, left):



21. From the **Touch UI Method** dropdown, select **Xerox Secure Access – Unified ID System**.
22. From the **Web UI Method** dropdown, select **User Name / Password – Validate on the Network**.
23. Click **Save**.
24. If an error about the device controller being asleep is displayed, then:



Operation Not Performed

The requested changes require the Network Controller be taken out of Sleep Mode. The button below can be used to start bringing the Network Controller out of Sleep Mode, which can take up to 20 seconds.

    a. Click the **Exit Sleep Mode** button.
    b. Wait for approximately 5 minutes for the device to respond (indicating that it is asleep).
    c. Print a test job.
    d. Log in to the device's web interface as an administrator.
    e. Click the **Touch UI Method** button.
    f. In **Touch UI Method**, select **Xerox Secure Access – Unified ID System**.
    g. In the **Web UI Method**, select **User Name / Password – Validate on the Network**.
    h. Click **Save**.

To verify the device's XSA authentication settings:

1. Access the physical device.
2. Log in as an administrator.
3. From the device's panel, run the Secure Access Settings Configuration Report.
4. Ensure the report accurately reflects the device's XSA authentication settings:
    a. **Server Name / IP Address** – The server name/ IP address of the PaperCut MF Application Server. For example, 10.100.66.75
    b. **Port Number** – 9192

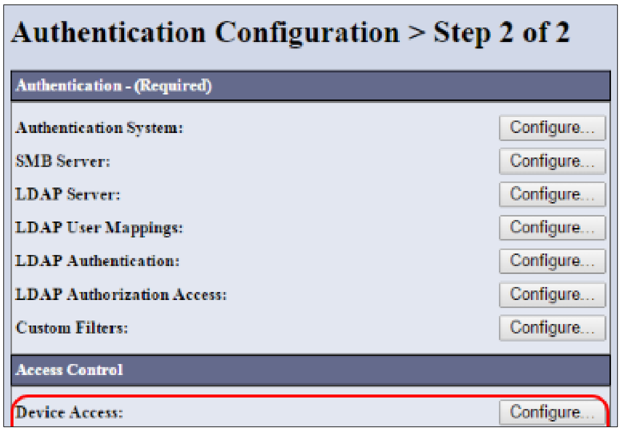
c. **Service Path** – "device/xerox-conv-auth/soap?deviceid=xxxx", where "xxxx" is an auto-generated device id. For example, " device/xerox-conv-auth/soap?deviceid=5005"
d. **Local Login** – Enabled
e. **Get Accounting Code** – Enabled

2.4.7 Configure the device’s user access permission settings

Note: This is only applicable to multi-function devices.

To configure the device’s user access permission settings to ensure that only authenticated users can access required device jobs:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > Login / Permissions / Accounting > User Permissions**.
3. In **User Permissions Roles**, click **Edit**.
4. In **non-logged in user**, click **Edit.**
5. Click **Services & Tools**.
6. In **Presets > Restrict access to all Services and Tools**, click **Apply**.
7. Navigate to **Properties > Security > Authentication Configuration > Next > Step 2 of 2**.
8. In **Access Control > Device Access**, click **Configure**.



Authentication Configuration > Step 2 of 2

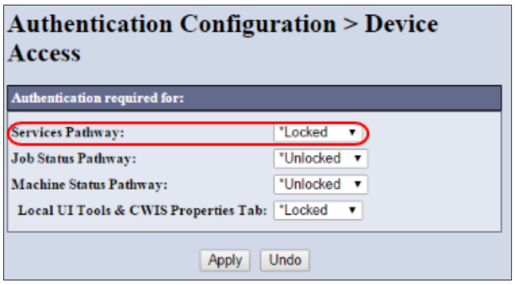
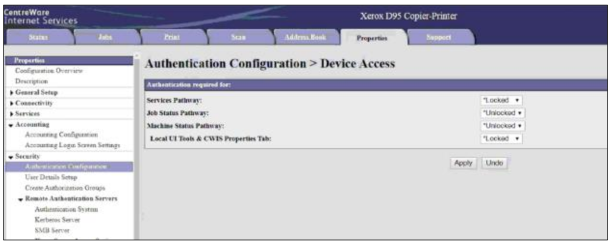
Authentication - (Required)

Authentication System: Configure...
SMB Server: Configure...
LDAP Server: Configure...
LDAP User Mappings: Configure...
LDAP Authentication: Configure...
LDAP Authorization Access: Configure...
Custom Filters: Configure...

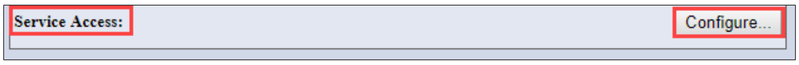
Access Control

Device Access: Configure...

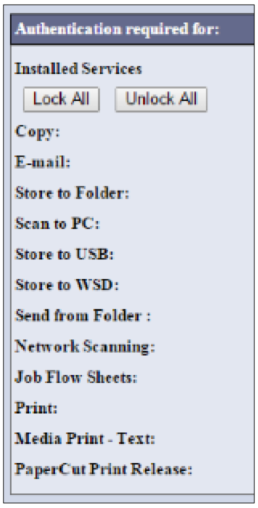
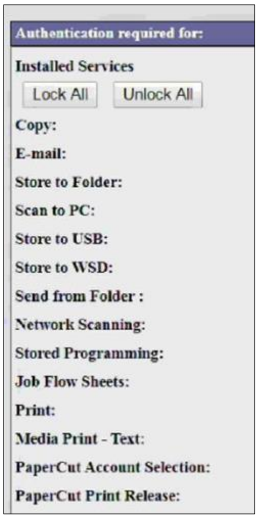
9. In **Services Pathway**, select **Locked**.
Note: This ensures that only authenticated users can access device jobs.

5325	D95
 Authentication Configuration > Device Access Authentication required for: Services Pathway: *Locked Job Status Pathway: *Unlocked Machine Status Pathway: *Unlocked Local UI Tools & CWIS Properties Tab: *Locked Apply Undo	 Authentication Configuration > Device Access Authentication required for: Services Pathway: *Locked Job Status Pathway: *Unlocked Machine Status Pathway: *Unlocked Local UI Tools & CWIS Properties Tab: *Locked Apply Undo

10. Navigate to **Properties > Security > Authentication Configuration > Next > Step 2 of 2**.
11. In **Access Control > Service Access**, click **Configure.**



Note: The list of all the available device jobs (**Installed Services**) are:

5325	D95
 Authentication required for: Installed Services Lock All Unlock All Copy: E-mail: Store to Folder: Scan to PC: Store to USB: Store to WSD: Send from Folder : Network Scanning: Job Flow Sheets: Print: Media Print - Text: PaperCut Print Release:	 Authentication required for: Installed Services Lock All Unlock All Copy: E-mail: Store to Folder: Scan to PC: Store to USB: Store to WSD: Send from Folder : Network Scanning: Stored Programming: Job Flow Sheets: Print: Media Print - Text: PaperCut Account Selection: PaperCut Print Release:

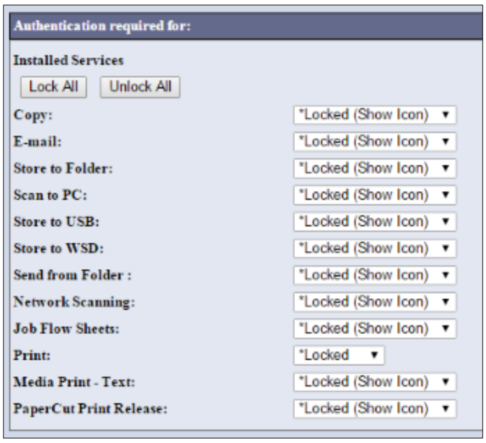
- Copy
- E-mail
- Store to Folder
- Scan to PC
- Store to USB
- Store to WSD
- Send from Folder
- Network Scanning
- Job Flow Sheets
- Print
- Media Print - Text
- PaperCut Print Release

For more information about each, consult the applicable third-party documentation available.

12. For each device job, select any one of the following:
    - **Unlocked** - This allows unauthenticated users to access the device job.
    - **Locked** - This allows only authenticated users to access the device job.

    Note: For **Print** and **PaperCut Print Release**, it is recommended that you select **Locked.**

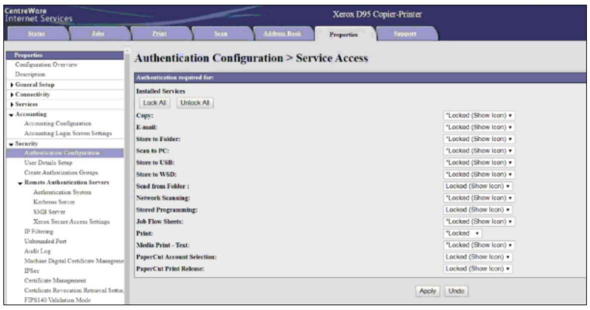
5325	D95



Authentication required for:

Installed Services

Copy:	*Locked (Show Icon)
E-mail:	*Locked (Show Icon)
Store to Folder:	*Locked (Show Icon)
Scan to PC:	*Locked (Show Icon)
Store to USB:	*Locked (Show Icon)
Store to WSD:	*Locked (Show Icon)
Send from Folder :	*Locked (Show Icon)
Network Scanning:	*Locked (Show Icon)
Job Flow Sheets:	*Locked (Show Icon)
Print:	*Locked
Media Print - Text:	*Locked (Show Icon)
PaperCut Print Release:	*Locked (Show Icon)



13. Click **Apply**.
14. Restart the device.

2.5 Setup procedure for ConnectKey 2.5 devices (EIP 3.0)

To set up PaperCut MF on ConnectKey 2.5 devices (running EIP 3.0), you must:

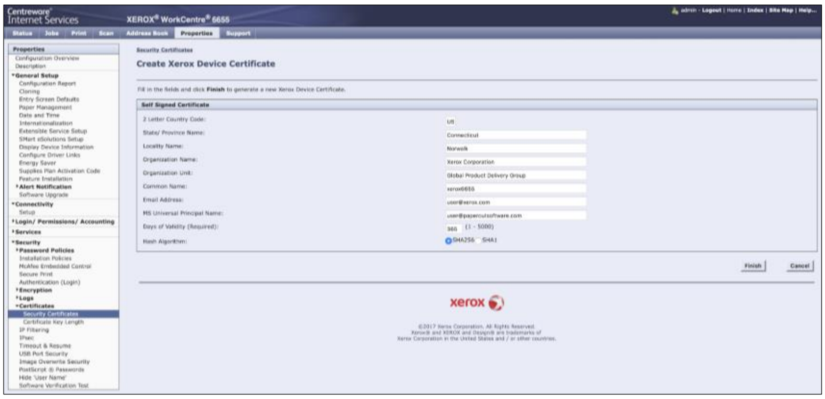
- 2.5.1 Configure the device’s security settings
- 2.5.2 Configure the device’s SNMP settings
- 2.5.3 Install PaperCut MF
- 2.5.4 Configure the device’s XSA authentication settings
- 2.5.5 Configure the device’s user access permission settings

Note: The navigation, instructions and images of the device and the device’s web interface are of ConnectKey 2.5 device, WC6655, running EIP 3.0. This could vary on other EIP 2.0-3.0 devices.

2.5.1 Configure the device’s security settings

To configure the device’s security settings:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > Security > Certificates > Security Certificates**.
3. Click **Create New Certificate**.
4. Enter the required details:



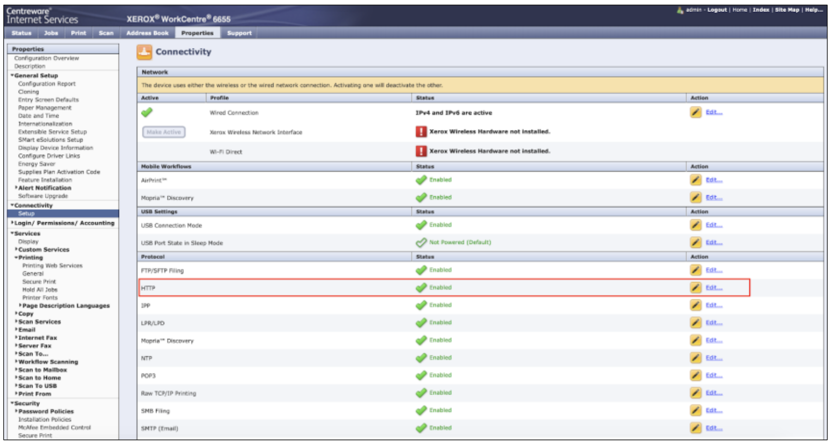
Create Xerox Device Certificate

Fill in the fields and click **Finish** to generate a new Xerox Device Certificate.

Self Signed Certificate

2 Letter Country Code:	US
State/ Province Name:	Connecticut
Locality Name:	Norwalk
Organization Name:	Xerox Corporation
Organization Unit:	Global Product Delivery Group
Common Name:	xerox6655
Email Address:	user@xerox.com
MS Universal Principal Name:	user@papercutsoftware.com
Days of Validity (Required):	365 (1 - 5000)
Hash Algorithm:	● SHA256 ○ SHA1

5. Click **Finish**.
6. Navigate to **Properties > Connectivity > Setup > Protocol > HTTP > Edit.**



Connectivity

Network

The device uses either the wireless or the wired network connection. Activating one will deactivate the other.

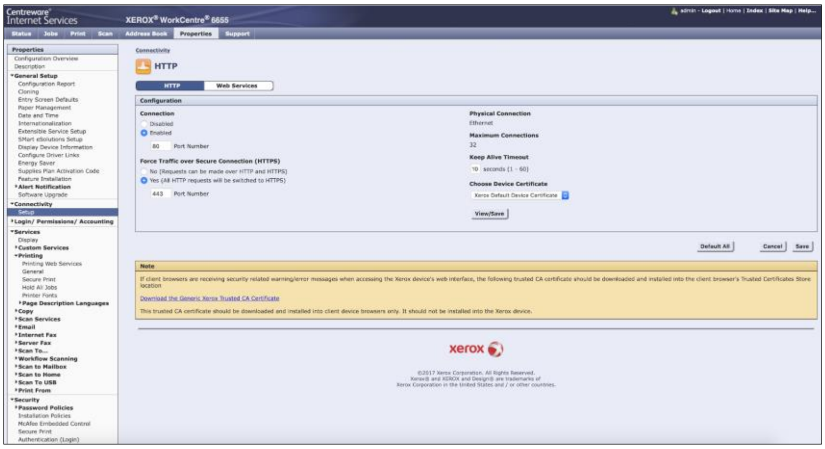
Active	Profile	Status	Action
✓	Wired Connection	IPv4 and IPv6 are active	Edit...
Make Active	Xerox Wireless Network Interface	Xerox Wireless Hardware not installed.	
	Wi-Fi Direct	Xerox Wireless Hardware not installed.	

Mobile Workflows	Status	Action
AirPrint™	Enabled	Edit...
Mopria™ Discovery	Enabled	Edit...

USB Settings	Status	Action
USB Connection Mode	Enabled	Edit...
USB Port State in Sleep Mode	Not Powered (Default)	Edit...

Protocol	Status	Action
FTP/SFTP Filing	Enabled	Edit...
HTTP	Enabled	Edit...
IPP	Enabled	Edit...
LPR/LPD	Enabled	Edit...
Mopria™ Discovery	Enabled	Edit...
NTP	Enabled	Edit...
POP3	Enabled	Edit...
Raw TCP/IP Printing	Enabled	Edit...
SMB Filing	Enabled	Edit...
SMTP (Email)	Enabled	Edit...

7. In **Connection**, select **Enabled.**
8. In **Force Traffic over Secure Connection (HTTPS)**, select **Yes.**



HTTP

Configuration

Connection
○ Disabled
● Enabled
80 Port Number

Force Traffic over Secure Connection (HTTPS)
○ No (Requests can be made over HTTP and HTTPS)
● Yes (All HTTP requests will be switched to HTTPS)
443 Port Number

Physical Connection
Ethernet

Maximum Connections
32

Keep Alive Timeout
10 seconds (1 - 60)

Choose Device Certificate
Xerox Default Device Certificate

Note

If client browsers are receiving security related warning/error messages when accessing the Xerox device's web interface, the following trusted CA certificate should be downloaded and installed into the client browser's Trusted Certificates Store location

Download the Generic Xerox Trusted CA Certificate

This trusted CA certificate should be downloaded and installed into client device browsers only. It should not be installed into the Xerox device.

9. Click **Save.**

2.5.2 Configure the device's SNMP settings

You can configure the device to use any one of the following SNMP settings:

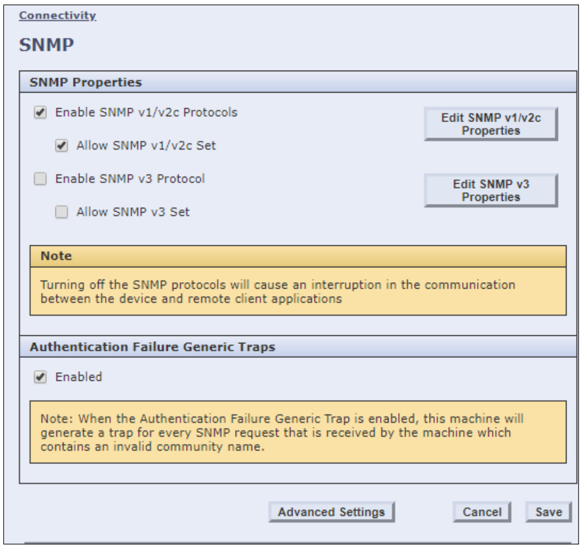
- 2.5.2.1 SNMPv1/v2c
- 2.5.2.2 SNMPv3

2.5.2.1 SNMPv1/v2c

To configure the device to use SNMPv1/v2c:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Connectivity > Setup > Protocol > SNMP**.

3. Select **Enable SNMP v1/v2c Protocols** and **Allow SNMP v1/v2c Set**:



Connectivity

SNMP

SNMP Properties

☑ Enable SNMP v1/v2c Protocols
  ☑ Allow SNMP v1/v2c Set
☐ Enable SNMP v3 Protocol
  ☐ Allow SNMP v3 Set

Note

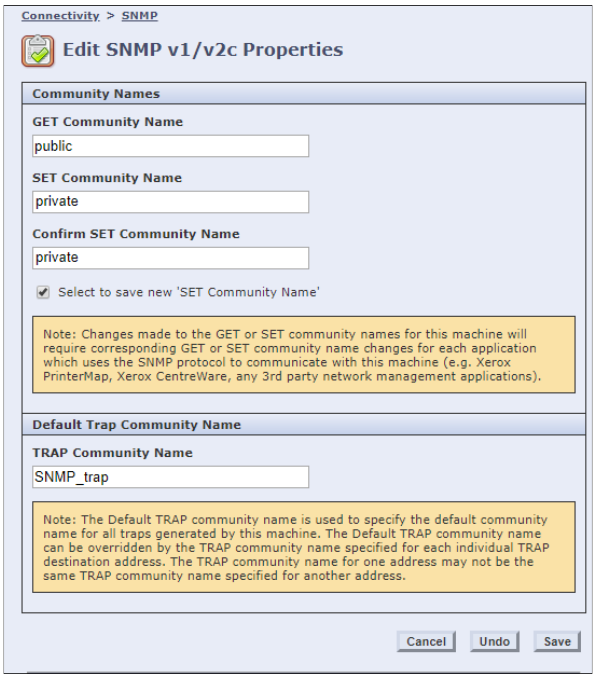
Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications

Authentication Failure Generic Traps

☑ Enabled

Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

4. Click **Edit SNMP v1/v2c Properties**.
5. In all the **Community Name** fields, enter relevant values:



Connectivity > SNMP

Edit SNMP v1/v2c Properties

Community Names

GET Community Name: public

SET Community Name: private

Confirm SET Community Name: private

☑ Select to save new 'SET Community Name'

Note: Changes made to the GET or SET community names for this machine will require corresponding GET or SET community name changes for each application which uses the SNMP protocol to communicate with this machine (e.g. Xerox PrinterMap, Xerox CentreWare, any 3rd party network management applications).

Default Trap Community Name

TRAP Community Name: SNMP_trap

Note: The Default TRAP community name is used to specify the default community name for all traps generated by this machine. The Default TRAP community name can be overridden by the TRAP community name specified for each individual TRAP destination address. The TRAP community name for one address may not be the same TRAP community name specified for another address.

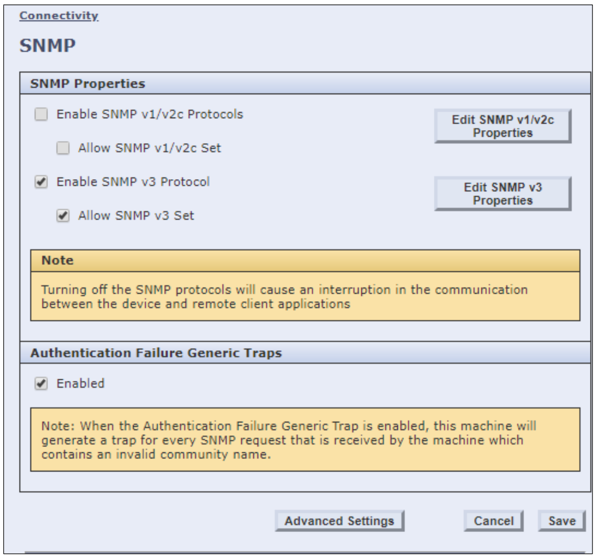
6. Take note of the **SET Community Name.**
7. Click **Save.**

2.5.2.2 SNMPv3

To configure the device to use SNMPv3:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties > Connectivity > Setup > Protocol > SNMP.**

3. Select **Enable SNMP v3 Protocol** and **Allow SNMP v3 Set**:



☐ Enable SNMP v1/v2c Protocols

☐ Allow SNMP v1/v2c Set

☑ Enable SNMP v3 Protocol

☑ Allow SNMP v3 Set

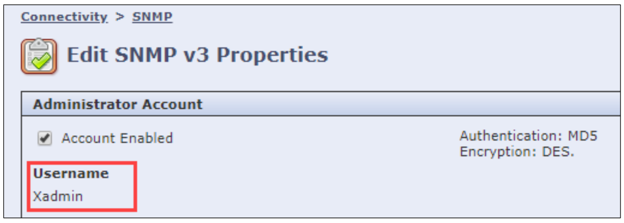
Note

Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications

☑ Enabled

Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

4. Click **Edit SNMP v3 Properties**.
5. In **Administrator Account**, select **Account Enabled**.
6. Take note of the **SNMP v3 Authentication Username/ Security Name:**

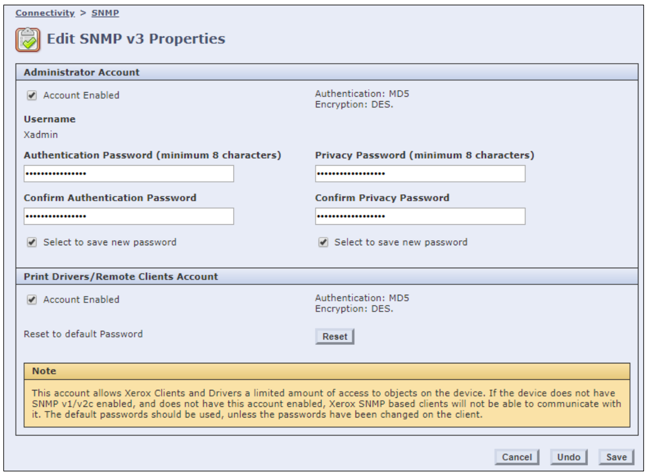


☑ Account Enabled

Authentication: MD5
Encryption: DES.

Username
Xadmin

7. In **Authentication Password** and **Privacy Password / Encryption Password**, enter relevant values:



☑ Account Enabled

Authentication: MD5
Encryption: DES.

Username
Xadmin

Authentication Password (minimum 8 characters): ••••••••••••••••

Privacy Password (minimum 8 characters): ••••••••••••••••••

Confirm Authentication Password: ••••••••••••••••

Confirm Privacy Password: ••••••••••••••••••

☑ Select to save new password

☑ Select to save new password

☑ Account Enabled

Authentication: MD5
Encryption: DES.

Reset to default Password

Note

This account allows Xerox Clients and Drivers a limited amount of access to objects on the device. If the device does not have SNMP v1/v2c enabled, and does not have this account enabled, Xerox SNMP based clients will not be able to communicate with it. The default passwords should be used, unless the passwords have been changed on the client.

8. Take note of the **Authentication Password** and the **Privacy Password / Encryption Password**.
9. Click **Save.**

2.5.3 Install PaperCut MF

To install PaperCut MF (i.e. device registration and integration):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.

3. In the **External Hardware Integration** area, select **Enable external hardware integration (for supported devices only)**.
4. Click **Apply**.
5. You can use any one of the following options:
    - 2.5.3.1 Install PaperCut MF on multiple devices
    - 2.5.3.2 Install PaperCut MF on each device

2.5.3.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 or above ships with a tool that can be run remotely to install PaperCut MF on multiple devices at once. Using this tool increases your operational efficiency by significantly reducing the time taken to install PaperCut MF. For more information, see the Enhanced Deployment Project.

2.5.3.2 Install PaperCut MF on each device

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

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**
4. In **Type**, select the applicable option, depending the device:
    - for multi-function devices, select **Xerox (Secure Access EIP 1.5+)**
    - for single function devices, select **Xerox (Secure Access EIP 1.5+) Print Only**
5. In **Device name**, enter a descriptive name for the device.
6. Optionally, in **Location/Department**, enter location or department details of the device.
7. In **Hostname / IP**, enter the network name or IP address of the device.
8. In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device's web interface.
9. To enable PaperCut MF to use:
    - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox is not selected (default).
    - SNMPv3, select the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox; and enter the following fields:
        - **Context name** – Do not enter any value.
        - **Username** – Enter **Xadmin**.
        - **Privacy password** – Enter the same value as the device web interface's **Privacy/ Encryption Password.**
        - **Authentication password** – Enter the same value as the device web interface's **Authentication Password.**
        - **Authentication protocol** – Select **MD5.**
        - **Privacy protocol** – Select **DES.**

    Note: For more information, see 4.5 SNMP.
10. In **Function**, select the required device jobs:

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

  Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.

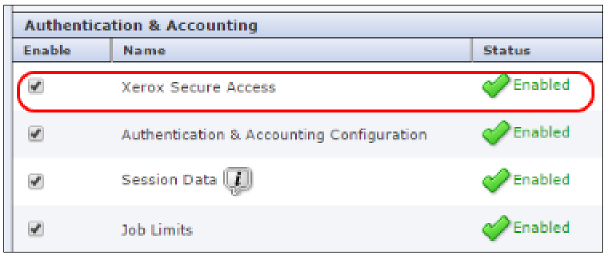
11. Click **Ok**.
12. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):
    - The PaperCut MF Admin web interface's **Device Status** displays the status **Started - Device is ready for user to login**.

2.5.4 Configure the device's XSA authentication settings

Note: This is only applicable to multi-function devices.

To configure the device's XSA authentication settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Login Methods > Web Service Enablement**.
3. Click **Edit**.
4. In **Xerox Secure Access**, select the checkbox (Enable).

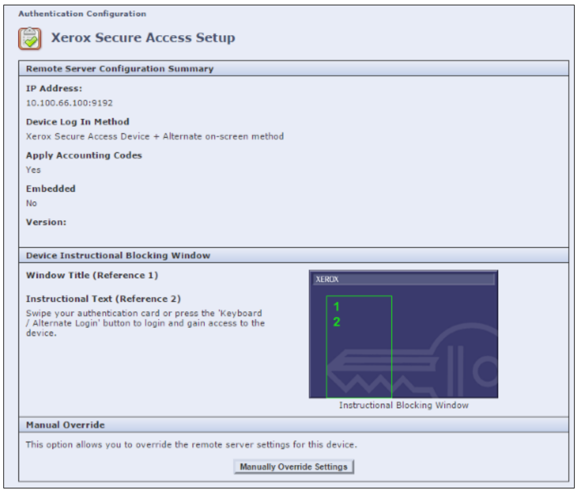


Authentication & Accounting

Enable	Name	Status
☑	Xerox Secure Access	✓ Enabled
☑	Authentication & Accounting Configuration	✓ Enabled
☑	Session Data	✓ Enabled
☑	Job Limits	✓ Enabled

To verify the device's XSA authentication settings:

1. Log in to the device's web interface as an administrator.
2. 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

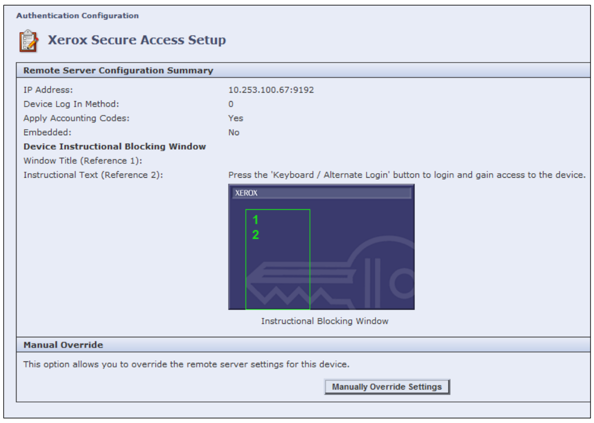
Window Title (Reference 1)

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

Manual Override

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

3. Click **Manually Override Settings**.



Authentication Configuration

Xerox Secure Access Setup

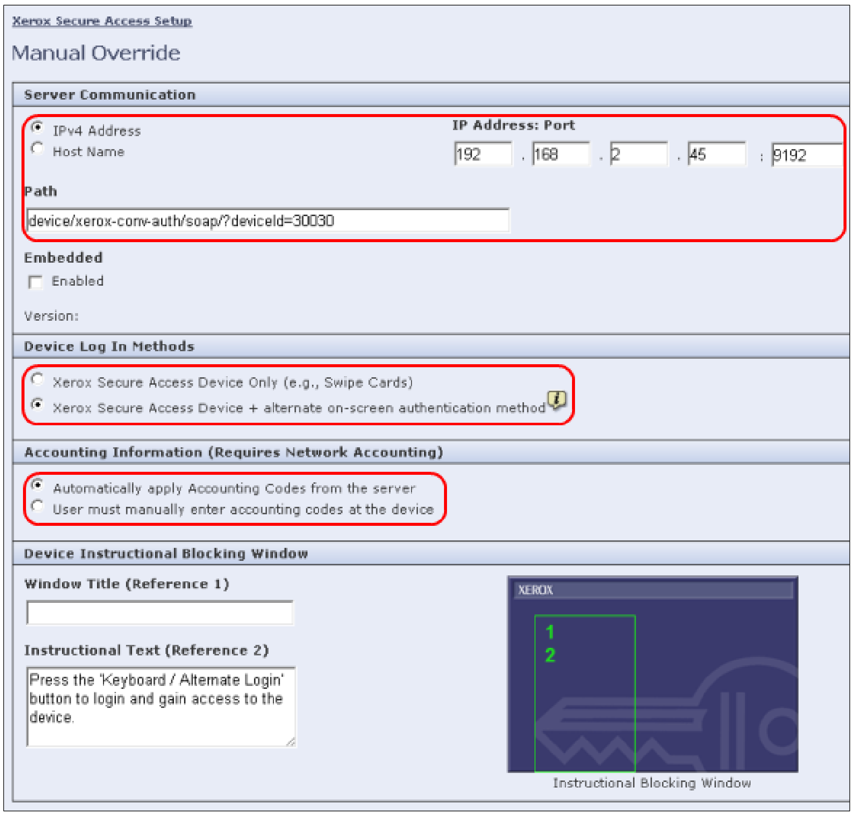
Remote Server Configuration Summary

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.

Manual Override

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

4. Ensure the device’s XSA authentication settings are accurately reflected:
    a. **IP Address** – The server name/ IP address of the PaperCut MF Application Server. For example, 10.100.66.75
    b. **Port** – 9192
    c. **Path** – "device/xerox-conv-auth/soap?deviceid=xxxx", where "xxxx" is an auto-generated device id. For example, " device/xerox-conv-auth/soap?deviceid=5005"
    d. **Xerox Secure Access Device + alternate on-screen authentication method** – Selected
    e. **Automatically apply Accounting Codes from the server** – Selected



Xerox Secure Access Setup

Manual Override

Server Communication

● IPv4 Address
○ Host Name

IP Address: Port: 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):

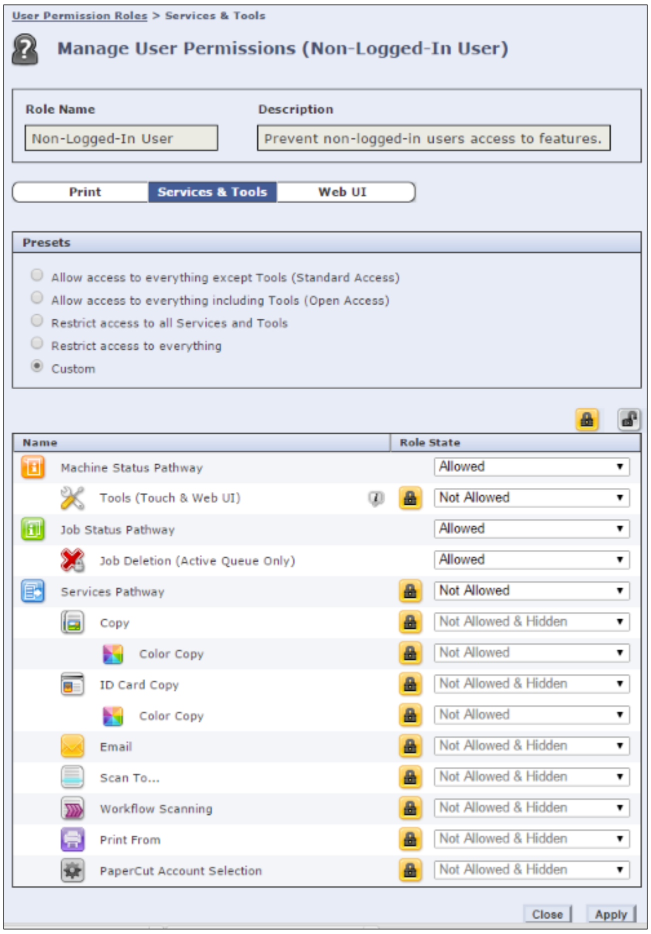
Instructional Text (Reference 2): Press the 'Keyboard / Alternate Login' button to login and gain access to the device.

2.5.5 Configure the device’s user access permission settings

Note: This is only applicable to multi-function devices.

To configure the device’s user access permission settings to ensure that only authenticated users can access required device jobs:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Login/Permissions/Accounting > User Permissions > User Permission Roles > Non-logged in Users > Edit > Services and Tools**.
3. For each device job, select any one of the following:
   - **Allowed** - This allows unauthenticated users to access the device job.
   - **Not Allowed** - This allows only authenticated users to access the device job.



Manage User Permissions (Non-Logged-In User)

Role Name: Non-Logged-In User

Description: Prevent non-logged-in users access to features.

Presets

○ Allow access to everything except Tools (Standard Access)
○ Allow access to everything including Tools (Open Access)
○ Restrict access to all Services and Tools
○ Restrict access to everything
● Custom

Name	Role State
Machine Status Pathway	Allowed
Tools (Touch & Web UI)	Not 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

4. Restart the device.

2.6 Setup procedure for VersaLink devices (EIP 3.7)

To set up PaperCut MF on VersaLink devices (running EIP 3.7), you must:

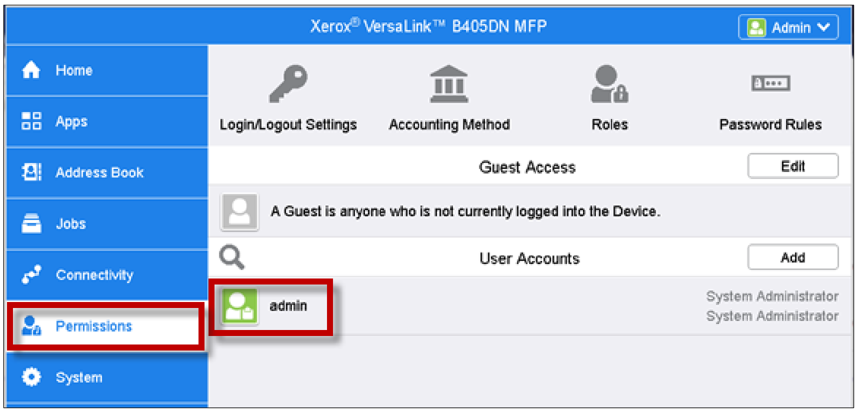
- 2.6.1 Configure the device web interface's administrator password
- 2.6.2 Configure the device's security settings
- 2.6.3 Configure the device's SNMP settings
- 2.6.4 Configure the device's accounting settings
- 2.6.5 Install PaperCut MF
- 2.6.6 Configure the device's XSA authentication settings
- 2.6.7 Configure the device's user access permission settings
- 2.6.8 Configure the device's walkup screen settings

Note: The navigation, instructions and images of the device and the device's web interface are of VersaLink device, B405, running EIP 3.7. This could vary on other EIP 3.7 devices.

2.6.1 Configure the device web interface's administrator password

To configure the device web interface's administrator password to configure the device's XSA authentication settings:

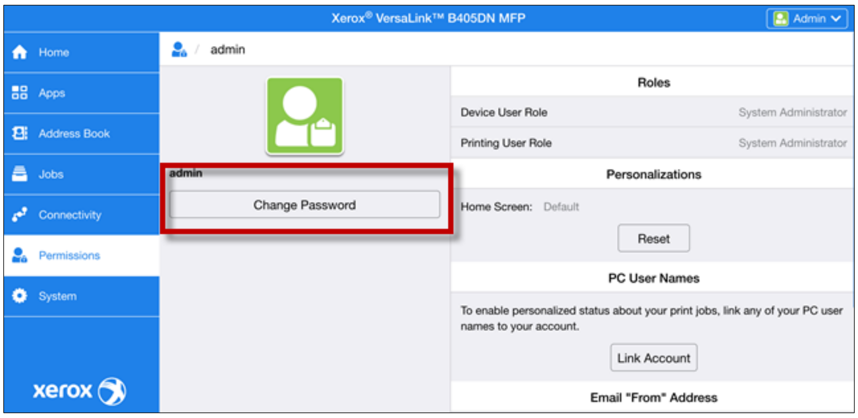
1. Log in to the device's web interface as an administrator.
2. Navigate to **Permissions > Login/Logout Settings > Admin**:



A Guest is anyone who is not currently logged into the Device.

admin — System Administrator, System Administrator

3. Click **Change Password**.



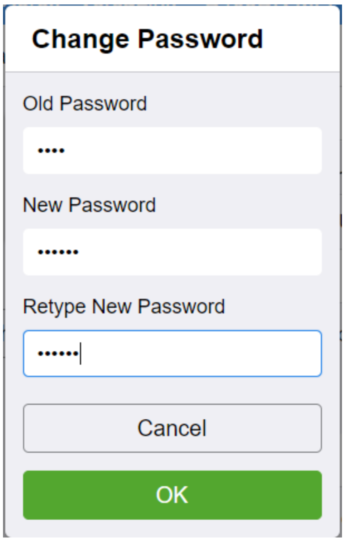
Device User Role: System Administrator

Printing User Role: System Administrator

Home Screen: Default

To enable personalized status about your print jobs, link any of your PC user names to your account.

4. Set the administrator credentials as required:



Old Password: ••••

New Password: ••••••

Retype New Password: ••••••

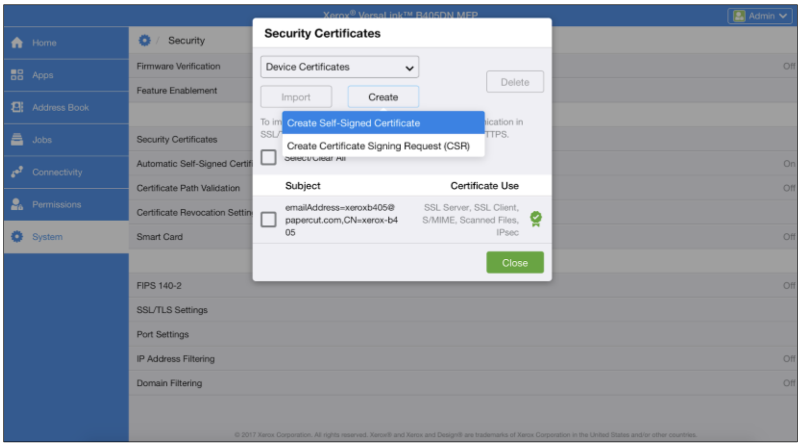
5. Click Ok.

6. Restart the device.

2.6.2 Configure the device's security settings

To configure the device's security settings:

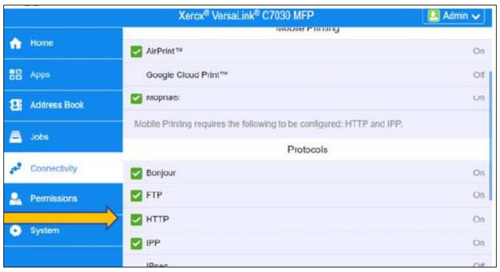
1. Log in to the device's web interface as an administrator.
2. Navigate to **System > Security > Security Certificates**.
3. Select **Device Certificates**.
4. Click **Create > Create Self-Signed Certificate**.


Xerox® VersaLink™ B405DN MFP
Admin
Home
Apps
Address Book
Jobs
Connectivity
Permissions
System
Security
Firmware Verification
Feature Enablement
Security Certificates
Automatic Self-Signed Certifi
Certificate Path Validation
Certificate Revocation Settin
Smart Card
FIPS 140-2
SSL/TLS Settings
Port Settings
IP Address Filtering
Domain Filtering
Security Certificates
Device Certificates
Import
Create
Delete
Create Self-Signed Certificate
Create Certificate Signing Request (CSR)
Select/Clear All
Subject
Certificate Use
Close
© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries.

Firmware Verification Off
Automatic Self-Signed Certifi On
Certificate Path Validation Off
Smart Card Off
FIPS 140-2 Off
IP Address Filtering Off
Domain Filtering Off

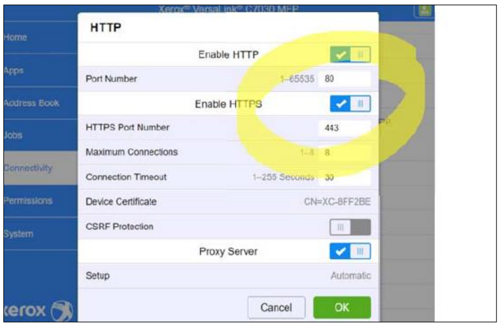
	Subject	Certificate Use
☐	emailAddress=xeroxb405@papercut.com,CN=xerox-b405	SSL Server, SSL Client, S/MIME, Scanned Files, IPsec

5. Enter the required details.
6. Click **Close**.
7. Navigate to **Connectivity > Protocols**
8. Select **HTTP.**



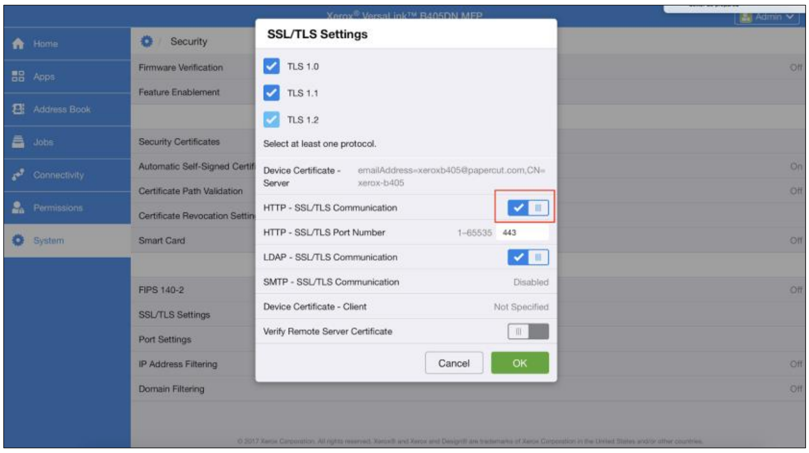
☑ AirPrint™ On
Google Cloud Print™ Off
☑ Mopria® On
Mobile Printing requires the following to be configured: HTTP and IPP.
☑ Bonjour On
☑ FTP On
☑ HTTP On
☑ IPP On
IPsec Off

9. Select **Enable HTTP** and **Enable HTTPS**; enter the relevant Port Numbers for HTTP and HTTPS.



Enable HTTP ☑
Port Number 1–65535 80
Enable HTTPS ☑
HTTPS Port Number 443
Maximum Connections 1–8 8
Connection Timeout 1–255 Seconds 30
Device Certificate CN=XC-8FF2BE
CSRF Protection ☐
Proxy Server ☑
Setup Automatic

10. Navigate to **System > Security > SSL/TLS Settings**.
11. Select **HTTP - SSL/TLS Communication**:



SSL/TLS Settings

☑ TLS 1.0

☑ TLS 1.1

☑ TLS 1.2

Select at least one protocol.

Device Certificate - Server: emailAddress=xeroxb405@papercut.com,CN=xerox-b405

HTTP - SSL/TLS Communication: ☑

HTTP - SSL/TLS Port Number: 1-65535 443

LDAP - SSL/TLS Communication: ☑

SMTP - SSL/TLS Communication: Disabled

Device Certificate - Client: Not Specified

Verify Remote Server Certificate: ☐

12. Click **Ok**.

2.6.3 Configure the device's SNMP settings

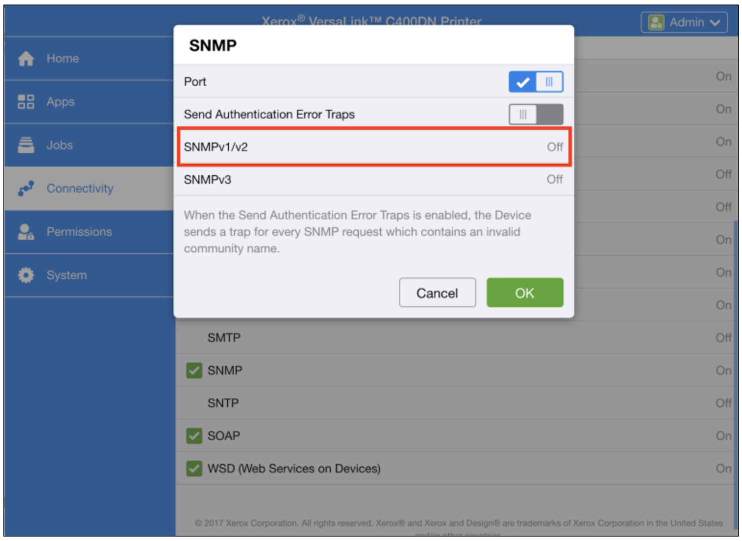
You can configure the device to use any one of the following SNMP settings:

- 2.6.3.1 SNMPv1/v2c
- 2.6.3.2 SNMPv3

2.6.3.1 SNMPv1/v2c

To configure the device to use SNMPv1/v2c:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Connectivity > Protocols > SNMP.**
3. Select **SNMPv1/v2**



SNMP

Port: ☑

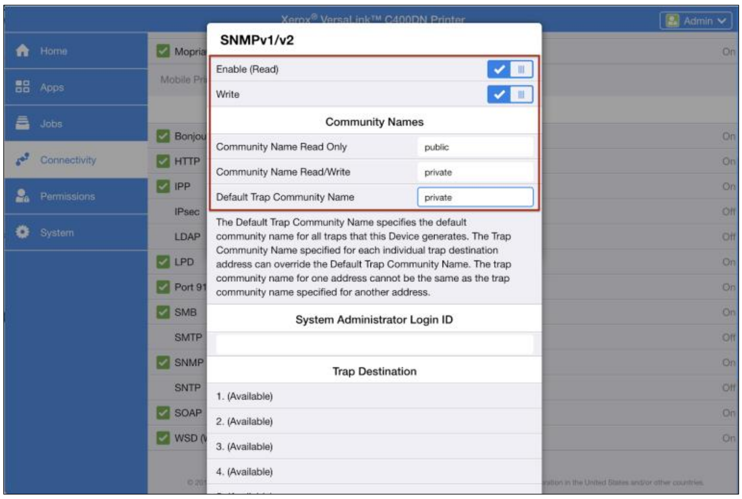
Send Authentication Error Traps: ☐

SNMPv1/v2: Off

SNMPv3: Off

When the Send Authentication Error Traps is enabled, the Device sends a trap for every SNMP request which contains an invalid community name.

4. Click **Edit SNMP v1/v2 Properties**.
5. Select **Enable (Read)** and **Write**.
6. In all the **Community Name** fields, enter relevant values:



SNMPv1/v2

Enable (Read) ☑

Write ☑

Community Names

Community Name Read Only	public
Community Name Read/Write	private
Default Trap Community Name	private

The Default Trap Community Name specifies the default community name for all traps that this Device generates. The Trap Community Name specified for each individual trap destination address can override the Default Trap Community Name. The trap community name for one address cannot be the same as the trap community name specified for another address.

System Administrator Login ID

Trap Destination

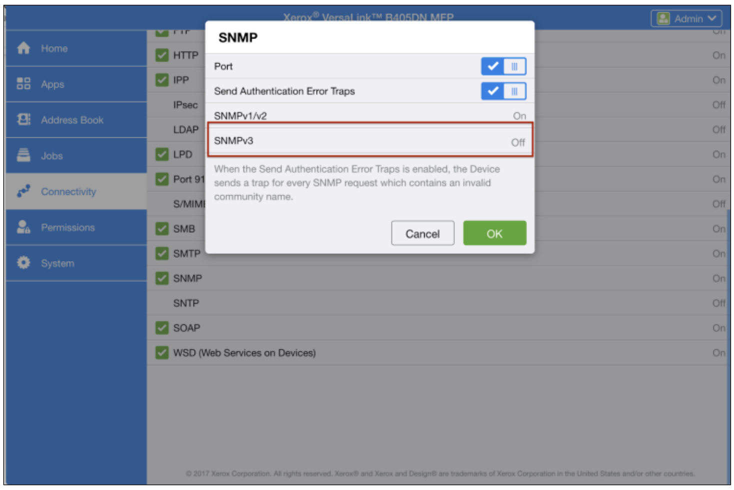
1. (Available)
2. (Available)
3. (Available)
4. (Available)

7. Take note of the **Community Name Read/Write.**
8. Click **Save.**

2.6.3.2 SNMPv3

To configure the device to use SNMPv3:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Connectivity > Protocols > SNMP.**
3. Select **SNMPv3.**


Xerox® VersaLink™ B405DN MFP
Admin
Home
Apps
Address Book
Jobs
Connectivity
Permissions
System
HTTP
IPP
IPsec
LDAP
LPD
Port 91
S/MIM
SMB
SMTP
SNMP
SNTP
SOAP
WSD (Web Services on Devices)
On
Off
Cancel
OK
© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries.

SNMP

Port ☑

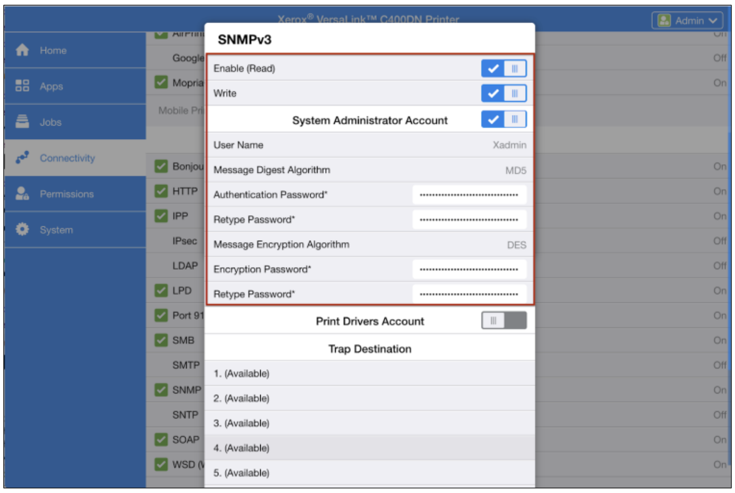
Send Authentication Error Traps ☑

SNMPv1/v2 On

SNMPv3 Off

When the Send Authentication Error Traps is enabled, the Device sends a trap for every SNMP request which contains an invalid community name.

4. Select **Enable (Read)** and **Write**.
5. Select **System Administrator Account**.
6. Take note of the **SNMP v3 Authentication Username**. For example, *Xadmin*.
7. In **Authentication Password** and **Privacy Password / Encryption Password**, enter relevant values:



SNMPv3

Enable (Read) ☑
Write ☑
System Administrator Account ☑
User Name: Xadmin
Message Digest Algorithm: MD5
Authentication Password*: ••••••••••••••••••••••••••••••••
Retype Password*: ••••••••••••••••••••••••••••••••
Message Encryption Algorithm: DES
Encryption Password*: ••••••••••••••••••••••••••••••••
Retype Password*: ••••••••••••••••••••••••••••••••
Print Drivers Account ☐

Trap Destination
1. (Available)
2. (Available)
3. (Available)
4. (Available)
5. (Available)

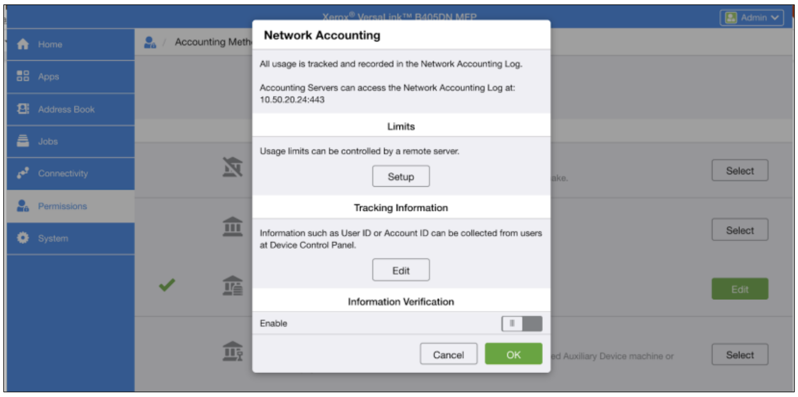
8. Take note of the **Authentication Password** and the **Privacy Password / Encryption Password**.

2.6.4 Configure the device’s accounting settings

Note: This is only applicable to multi-function devices.

To configure the device’s accounting settings to ensure that jobs are accurately logged:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Permissions > Accounting Method > Network > Edit > Limits > Setup**.



Network Accounting

All usage is tracked and recorded in the Network Accounting Log.

Accounting Servers can access the Network Accounting Log at:
10.50.20.24:443

Limits

Usage limits can be controlled by a remote server.

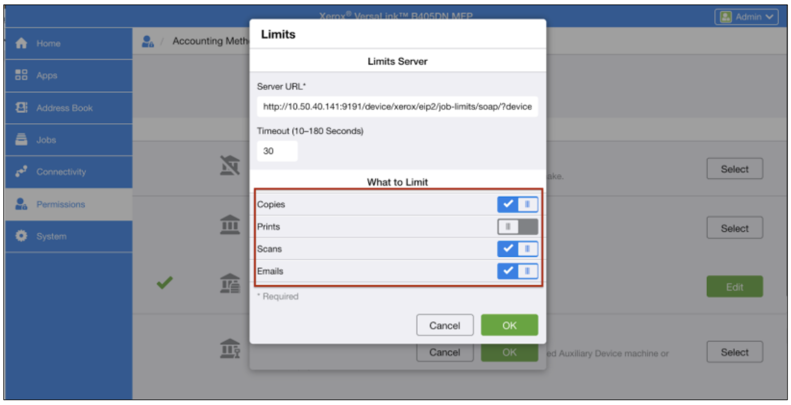
Tracking Information

Information such as User ID or Account ID can be collected from users at Device Control Panel.

Information Verification

Enable ☐

3. Select **Copies, Scans** and **Emails.**



Limits

Limits Server

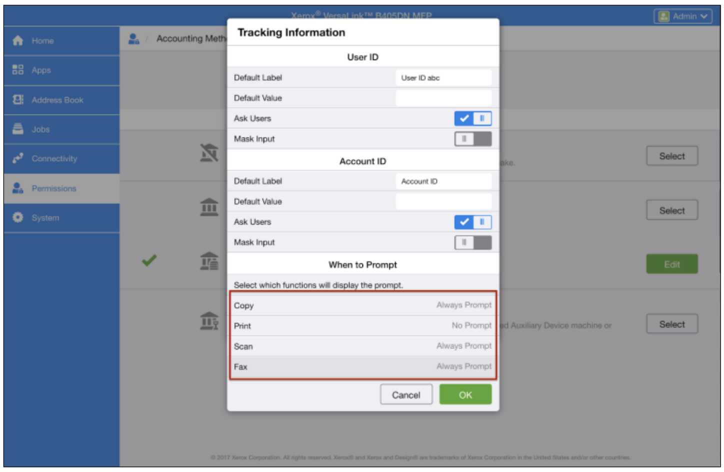
Server URL*: http://10.50.40.141:9191/device/xerox/eip2/job-limits/soap/?device

Timeout (10–180 Seconds): 30

What to Limit
Copies ☑
Prints ☐
Scans ☑
Emails ☑

* Required

4. Click **OK**.
5. Navigate to **Permissions > Accounting Method > Network > Edit > Tracking Information > Edit.**
6. In **When to Prompt** (Copy, Scan, Fax), select **Always Prompt**.



Tracking Information

User ID
Default Label: User ID abc
Default Value:
Ask Users: ☑
Mask Input: ☐

Account ID
Default Label: Account ID
Default Value:
Ask Users: ☑
Mask Input: ☐

When to Prompt
Select which functions will display the prompt.
Copy: Always Prompt
Print: No Prompt
Scan: Always Prompt
Fax: Always Prompt

7. Restart the device.

2.6.5 Install PaperCut MF

To install PaperCut MF (i.e. device registration and integration):

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

2.6.5.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 or above ships with a tool that can be run remotely to install PaperCut MF on multiple devices in bulk. Using this tool increases your operational efficiency by significantly reducing the time taken to install PaperCut MF. For more information, see the Enhanced Deployment Project.

2.6.5.2 Install PaperCut MF on each device

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

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**
4. In **Type**, select the applicable option, depending the device:
   - for multi-function devices, select **Xerox (Secure Access EIP 1.5+)**
   - for single function devices, select **Xerox (Secure Access EIP 1.5+) Print Only**
5. In **Device name**, enter a descriptive name for the device.
6. Optionally, in **Location/Department**, enter location or department details of the device.
7. In **Hostname / IP**, enter the network name or IP address of the device.

8. In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device's web interface.
9. To enable PaperCut MF to use:
    - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox is not selected (default).
    - SNMPv3, select the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox; and enter the following fields:
        - **Context name** – Do not enter any value.
        - **Username** – Enter **Xadmin**.
        - **Privacy password** – Enter the same value as the device web interface's **Privacy/ Encryption Password.**
        - **Authentication password** – Enter the same value as the device web interface's **Authentication Password.**
        - **Authentication protocol** – Select **MD5.**
        - **Privacy protocol** – Select **DES.**

    Note: For more information, see 4.5 SNMP.
10. In **Function**, select the required device jobs:
    - **Track & control copying**
    - **Track & control scanning**
    - **Track & control faxing**
    - **Enable print release**

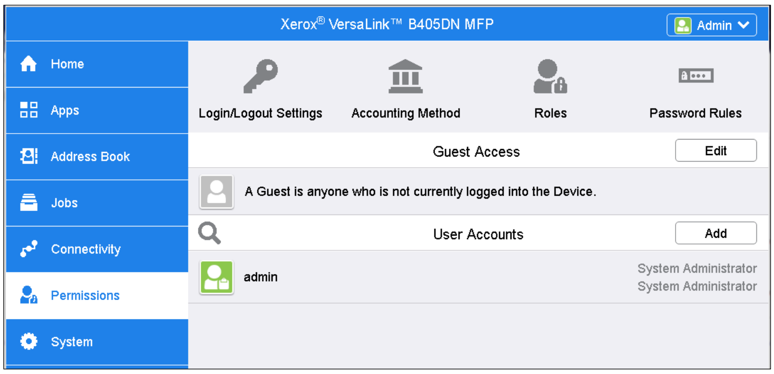
    Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.
11. Click **Ok**.
12. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):
    - The PaperCut MF Admin web interface's **Device Status** displays the status **Started - Device is ready for user to login**.

2.6.6 Configure the device's XSA authentication settings

Note: This is only applicable to multi-function devices.

To configure the device's XSA authentication settings:

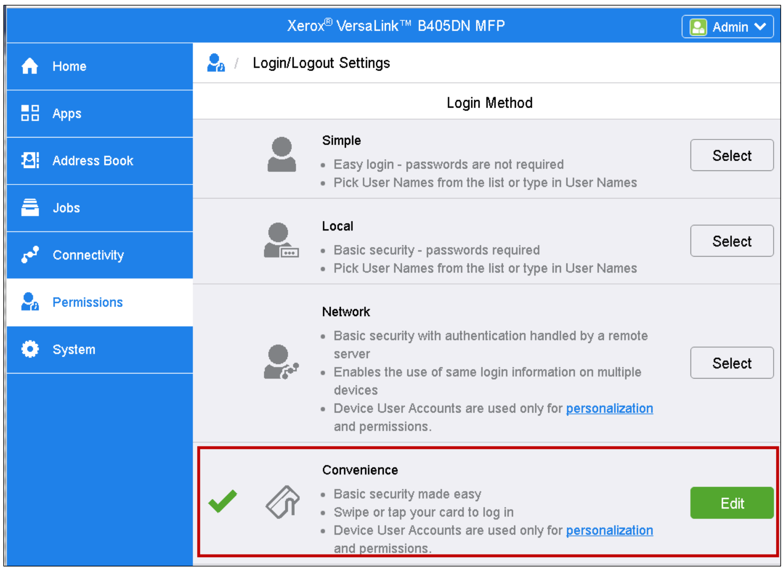
1. Log in to the device's web interface as an administrator.
2. Ensure to change the device web interface's default administrator password. For more information, 2.6.1 Configure the device web interface's administrator password.
3. Navigate to **Permissions > Login/Logout Settings**.



A Guest is anyone who is not currently logged into the Device.

admin — System Administrator, System Administrator

4. In **Convenience**, click **Edit**.



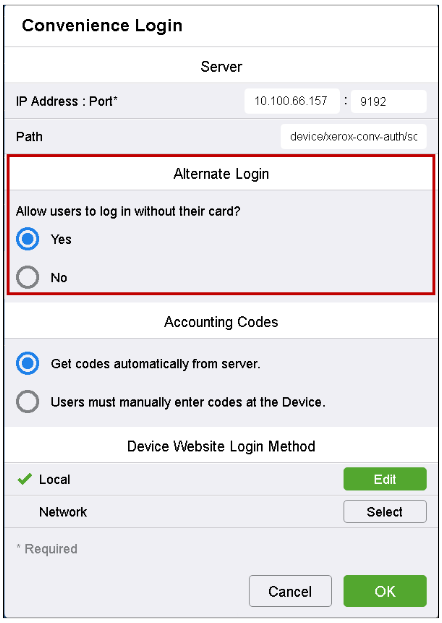
Simple
- Easy login - passwords are not required
- Pick User Names from the list or type in User Names

Local
- Basic security - passwords required
- Pick User Names from the list or type in User Names

Network
- Basic security with authentication handled by a remote server
- Enables the use of same login information on multiple devices
- Device User Accounts are used only for personalization and permissions.

✓ Convenience
- Basic security made easy
- Swipe or tap your card to log in
- Device User Accounts are used only for personalization and permissions.

5. In **Allow users to log in without their card?**, select **Yes**.



IP Address : Port* 10.100.66.157 : 9192

Path device/xerox-conv-auth/sc

Allow users to log in without their card?

● Yes

○ No

● Get codes automatically from server.

○ Users must manually enter codes at the Device.

✓ Local

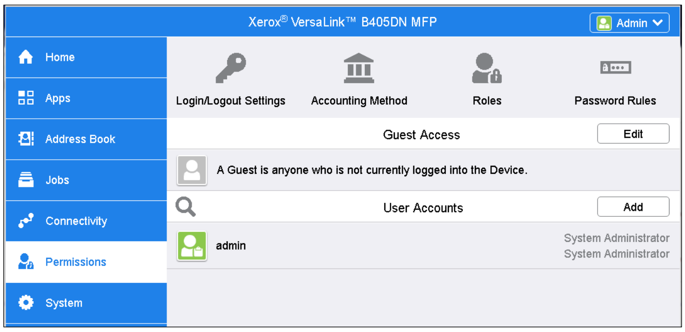
Network

* Required

6. Click **Ok**.
7. Restart the device.

To verify the device's XSA authentication settings:

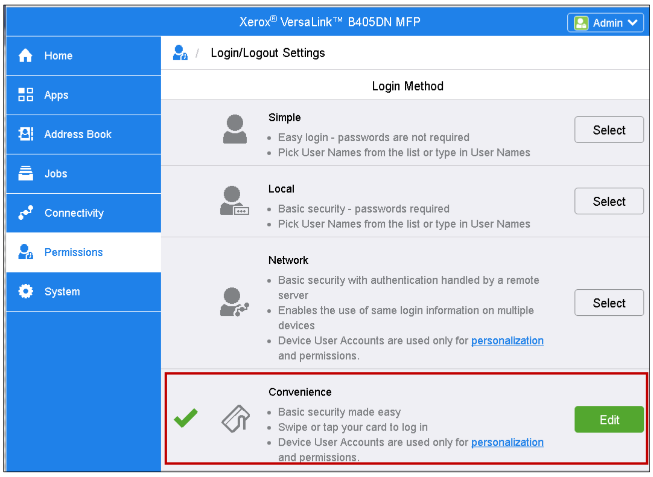
1. Log in to the device's web interface as an administrator.
2. Navigate to **Permissions > Login/Logout Settings**.



A Guest is anyone who is not currently logged into the Device.

admin — System Administrator, System Administrator

3. In **Convenience**, click **Edit**.



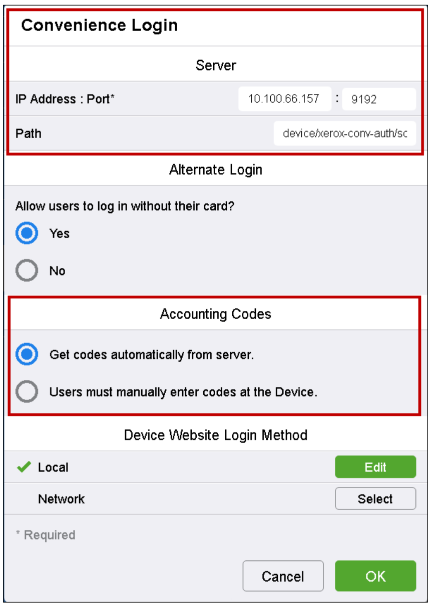
Simple
- Easy login - passwords are not required
- Pick User Names from the list or type in User Names

Local
- Basic security - passwords required
- Pick User Names from the list or type in User Names

Network
- Basic security with authentication handled by a remote server
- Enables the use of same login information on multiple devices
- Device User Accounts are used only for personalization and permissions.

✓ Convenience
- Basic security made easy
- Swipe or tap your card to log in
- Device User Accounts are used only for personalization and permissions.

4. Ensure the device's XSA authentication settings are accurately reflected:
    a. **IP Address** – The server name/ IP address of the PaperCut MF Application Server. For example, 10.100.66.75
    b. **Port** – 9192
    c. **Path** – "device/xerox-conv-auth/soap?deviceid=xxxx", where "xxxx" is an auto-generated device id. For example, " device/xerox-conv-auth/soap?deviceid=5005"
    d. **Get codes automatically from server** – Selected



IP Address : Port* 10.100.66.157 : 9192

Path device/xerox-conv-auth/sc

Allow users to log in without their card?

● Yes

○ No

● Get codes automatically from server.

○ Users must manually enter codes at the Device.

✓ Local

Network

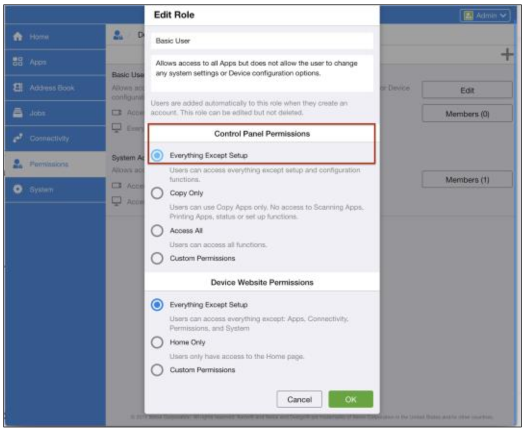
* Required

2.6.7 Configure the device's user access permission settings

Note: This is only applicable to multi-function devices.

To configure the device's user access permission settings to ensure that only authenticated users can access required device jobs:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Permissions > Roles > Device User Roles.**
3. Select any one of the following:
    - **Everything Except Setup** - This allows unauthenticated users to access all relevant device jobs.



Edit Role

Basic User

Allows access to all Apps but does not allow the user to change any system settings or Device configuration options.

Users are added automatically to this role when they create an account. This role can be edited but not deleted.

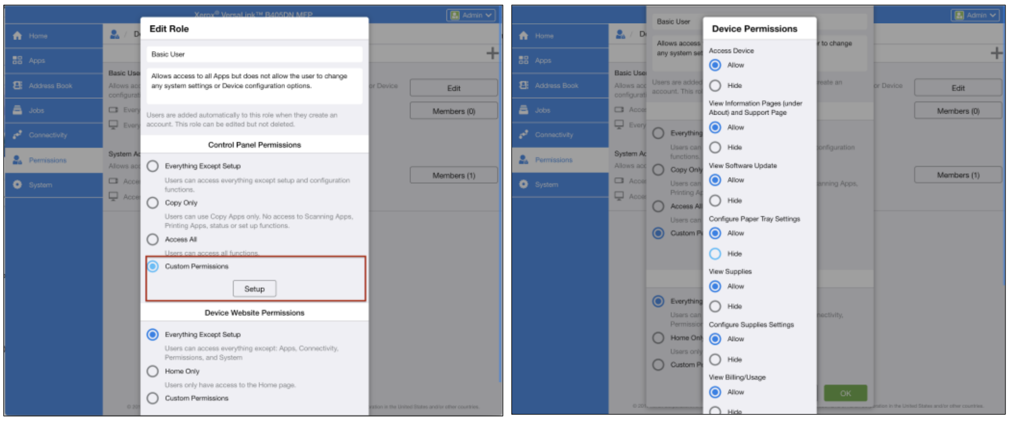
Control Panel Permissions

● Everything Except Setup
Users can access everything except setup and configuration functions.
○ Copy Only
Users can use Copy Apps only. No access to Scanning Apps, Printing Apps, status or set up functions.
○ Access All
Users can access all functions.
○ Custom Permissions

Device Website Permissions

● Everything Except Setup
Users can access everything except: Apps, Connectivity, Permissions, and System
○ Home Only
Users only have access to the Home page.
○ Custom Permissions

    - **Custom Permissions > Setup** > **Device Permissions** - This allows only authenticated users to access each device job specified.



Edit Role

Basic User

Control Panel Permissions

○ Everything Except Setup
○ Copy Only
○ Access All
● Custom Permissions

Device Website Permissions

● Everything Except Setup
○ Home Only
○ Custom Permissions

Device Permissions

Access Device
● Allow
○ Hide

View Information Pages (under About) and Support Page
● Allow
○ Hide

View Software Update
● Allow
○ Hide

Configure Paper Tray Settings
● Allow
○ Hide

View Supplies
● Allow
○ Hide

Configure Supplies Settings
● Allow
○ Hide

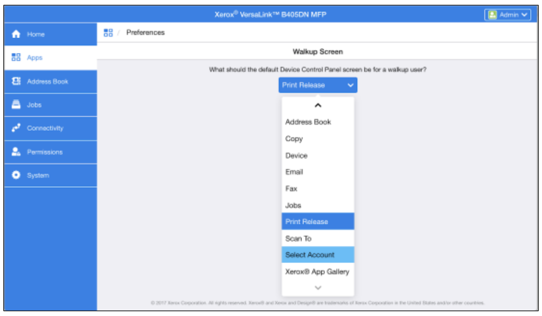
View Billing/Usage
● Allow
○ Hide

4. Restart the device.

2.6.8 Configure the device's walkup screen settings

To configure the device's walkup screen settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Apps > Preferences > Walkup Screen.**
3. In **What should the default Device Control Panel screen be for a walkup user?** select either **Print Release** or **Select Account**.



Walkup Screen

What should the default Device Control Panel screen be for a walkup user?

Print Release

2.7 Setup procedure for AltaLink devices (EIP 4.0)

To set up PaperCut MF on AltaLink devices (running EIP 4.0), you must:

- 2.7.1 Install PaperCut MF
- 2.7.2 Configure the device's XSA authentication settings
- 2.7.3 Configure the device's user access permission settings

Note: The navigation, instructions and images of the device and the device's web interface are of VersaLink device, C8070, running EIP 4.0. This could vary on other EIP 4.0 devices.

2.7.1 Install PaperCut MF

To install PaperCut MF (i.e. device registration and integration):

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

2.7.1.1 Install PaperCut MF on multiple devices

PaperCut MF 19.2.0 or above ships with a tool that can be run remotely to install PaperCut MF on multiple devices at once. Using this tool increases your operational efficiency by significantly reducing the time taken to install PaperCut MF. For more information, see the Enhanced Deployment Project.

2.7.1.2 Install PaperCut MF on each device

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

To install PaperCut MF on each device:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**

4. In **Type**, select the applicable option, depending the device:
    - for multi-function devices, select **Xerox (Secure Access EIP 1.5+)**
    - for single function devices, select **Xerox (Secure Access EIP 1.5+) Print Only**
5. In **Device name**, enter a descriptive name for the device.
6. Optionally, in **Location/Department**, enter location or department details of the device.
7. In **Hostname / IP**, enter the network name or IP address of the device.
8. In **Device's administrator username** and **Device's administrator password**, enter the same administrator credentials (username and password) used for the device's web interface.
9. To enable PaperCut MF to use:
    - SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox is not selected (default).
    - SNMPv3, select the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox; and enter the following fields:
        - **Context name** – Do not enter any value.
        - **Username** – Enter **Xadmin**.
        - **Privacy password** – Enter the same value as the device web interface's **Privacy/ Encryption Password.**
        - **Authentication password** – Enter the same value as the device web interface's **Authentication Password.**
        - **Authentication protocol** – Select **MD5.**
        - **Privacy protocol** – Select **DES.**

    Note: For more information, see 4.5 SNMP.
10. In **Function**, select the required device jobs:
    - **Track & control copying**
    - **Track & control scanning**
    - **Track & control faxing**
    - **Enable print release**

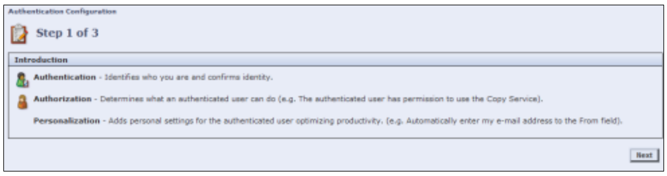
    Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.
11. Click **Ok**.
12. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):
    - The PaperCut MF Admin web interface's **Device Status** displays the status **Started - Device is ready for user to login**.

2.7.2 Configure the device's XSA authentication settings

Note: This is only applicable to multi-function devices.

To configure the device's XSA authentication settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Security > Authentication Configuration > Next**

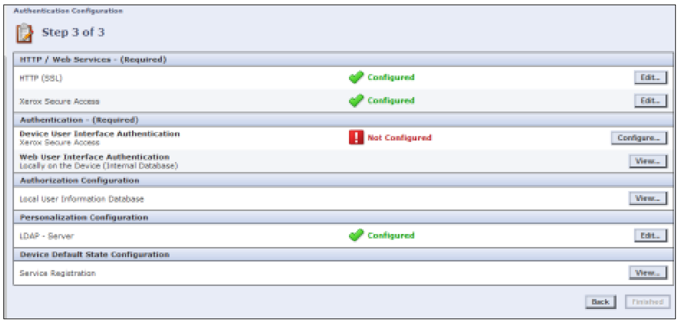


Authentication - Identifies who you are and confirms identity.

Authorization - Determines what an authenticated user can do (e.g. The authenticated user has permission to use the Copy Service).

Personalization - Adds personal settings for the authenticated user optimizing productivity. (e.g. Automatically enter my e-mail address to the From field).

3. In **Device User Interface Authentication**, click **Configure**.

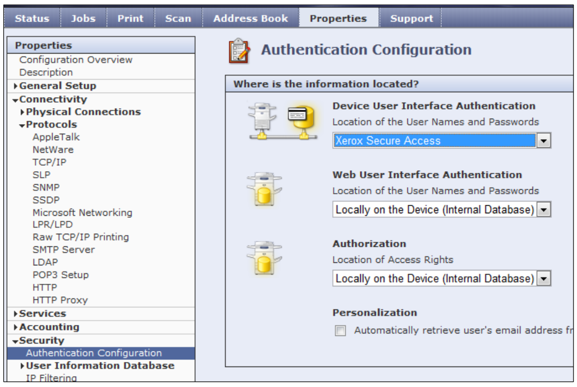


Authentication Configuration

Step 3 of 3

HTTP / Web Services - (Required)		
HTTP (SSL)	✓ Configured	Edit...
Xerox Secure Access	✓ Configured	Edit...
Authentication - (Required)		
Device User Interface Authentication Xerox Secure Access	! Not Configured	Configure...
Web User Interface Authentication Locally on the Device (Internal Database)		View...
Authorization Configuration		
Local User Information Database		View...
Personalization Configuration		
LDAP - Server	✓ Configured	Edit...
Device Default State Configuration		
Service Registration		View...

4. In **Device User Interface Authentication**, select **Xerox Secure Access**:



Authentication Configuration

Where is the information located?

Device User Interface Authentication
Location of the User Names and Passwords
Xerox Secure Access

Web User Interface Authentication
Location of the User Names and Passwords
Locally on the Device (Internal Database)

Authorization
Location of Access Rights
Locally on the Device (Internal Database)

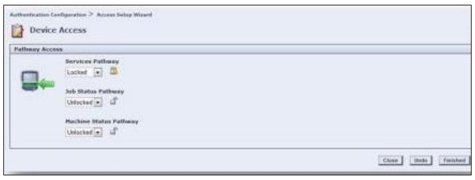
Personalization
☐ Automatically retrieve user's email address fr

2.7.3 Configure the device's user access permission settings

Note: This is only applicable to multi-function devices.

To configure the device's user access permission settings to ensure that only authenticated users can access required device jobs:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties > Security > Authentication Configuration > Device Access**.
3. In **Services Pathway** or for each device job, select any one of the following:
   - **Unlocked** - This allows unauthenticated users to access the device job.
   - **Locked** - This allows only authenticated users to access the device job.



Authentication Configuration > Access Setup Wizard

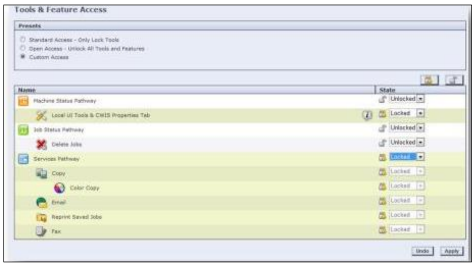
Device Access

Pathway Access

Services Pathway: Locked

Job Status Pathway: Unlocked

Machine Status Pathway: Unlocked



Tools & Feature Access

Presets

○ Standard Access - Only Lock Tools
○ Open Access - Unlock All Tools and Features
● Custom Access

Name	State
Machine Status Pathway	Unlocked
Local UI Tools & CWIS Properties Tab	Locked
Job Status Pathway	Unlocked
Delete Jobs	Unlocked
Services Pathway	Locked
Copy	Locked
Color Copy	Locked
Email	Locked
Reprint Saved Jobs	Locked
Fax	Locked

4. Restart the device.

2.8 Setup procedure for AltaLink C8100 (series) & EC8000 (series) devices (EIP 4.0+)

To set up PaperCut MF on Xerox AltaLink 8100 series & Xerox EC8000 series devices (running EIP 4.0+), you must:

- 2.8.1 Install PaperCut MF (version 20.0.4 or later to prevent compatibility issues)

1. 2.8.2 Enable all EIP Web Services

- Configure the device's Date and Time settings
- 2.8.4 Configure the device's User Permission Roles settings

Note: The navigation, instructions and images of the device and the device's web interface are from a Xerox AltaLink C8155, running EIP 4.0. This could vary on other EIP 4.0 devices.

Additional troubleshooting instructions for these devices can be found in 2.8.6 Troubleshooting installation.

2.8.1 Install PaperCut MF

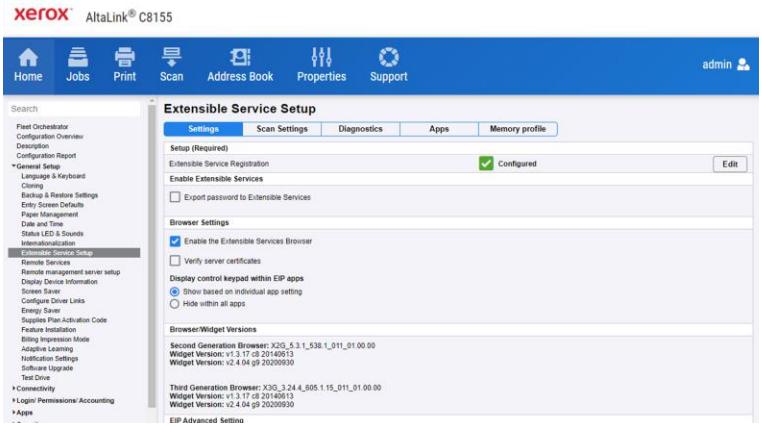
To install PaperCut MF (i.e. device registration and integration):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **External Hardware Integration** area, select **Enable external hardware integration (for supported devices only)**.
4. Click **Apply**.
5. You can use one of the following options:
    - 2.7.1.1 Install PaperCut MF on multiple devices
    - 2.7.1.2 Install PaperCut MF on each device (if running Papercut 19.2.0 or prior)

2.8.2 Enable all EIP Web Services

To configure the device’s EIP Web Services:

2. Log in to the device’s web interface as an administrator.
3. Navigate to **Properties (tab) > General Setup > Extensible Service Setup > Extensible Service Registration,** select **Edit** then **Enable All** and press **Save**.



Extensible Service Setup

Setup (Required)

Extensible Service Registration ✓ Configured

Enable Extensible Services

☐ Export password to Extensible Services

Browser Settings

☑ Enable the Extensible Services Browser

☐ Verify server certificates

Display control keypad within EIP apps

● Show based on individual app setting

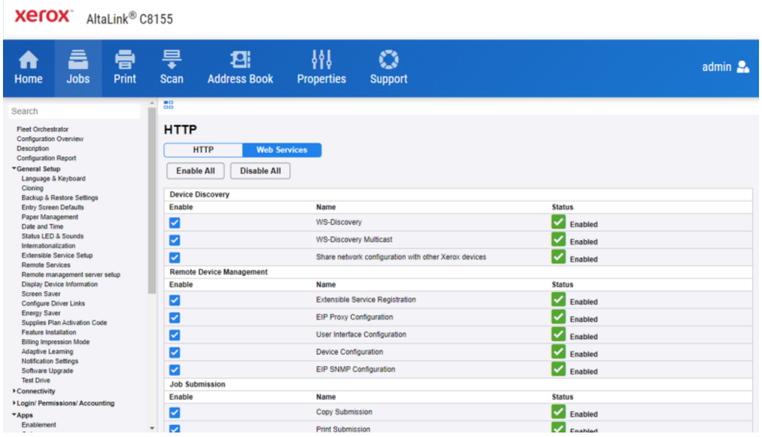
○ Hide within all apps

Browser/Widget Versions

Second Generation Browser: X2G_5.3.1_538.1_011_01.00.00
Widget Version: v1.3.17 c8 20140613
Widget Version: v2.4.04 g9 20200930

Third Generation Browser: X3G_3.24.4_605.1.15_011_01.00.00
Widget Version: v1.3.17 c8 20140613
Widget Version: v2.4.04 g9 20200930

EIP Advanced Setting



HTTP

Device Discovery

Enable	Name	Status
☑	WS-Discovery	✓ Enabled
☑	WS-Discovery Multicast	✓ Enabled
☑	Share network configuration with other Xerox devices	✓ Enabled

Remote Device Management

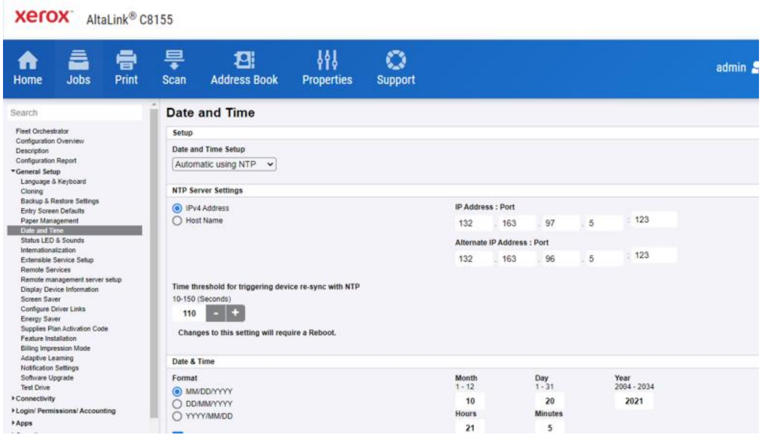
Enable	Name	Status
☑	Extensible Service Registration	✓ Enabled
☑	EIP Proxy Configuration	✓ Enabled
☑	User Interface Configuration	✓ Enabled
☑	Device Configuration	✓ Enabled
☑	EIP SNMP Configuration	✓ Enabled

Job Submission

Enable	Name	Status
☑	Copy Submission	✓ Enabled
☑	Print Submission	✓ Enabled

2.8.3 Configure the device's Date and Time settings

1. Log in to the device's web interface as an administrator.
2. Ensure the device's Date and Time are synchronised to the same NTP server as the PaperCut MF Application Server or ensure the time settings on the PaperCut MF Application server match the device's Date and Time settings.
    a. Navigate to **Properties (tab) > General Setup > Date and Time**
    b. When using a NTP server, specify the NTP server and ensure the NTP server matches the NTP server used on the PaperCut MF Application Server.



Date and Time

Setup

Date and Time Setup: Automatic using NTP

NTP Server Settings

● IPv4 Address
○ Host Name

IP Address : Port: 132 . 163 . 97 . 5 : 123

Alternate IP Address : Port: 132 . 163 . 96 . 5 : 123

Time threshold for triggering device re-sync with NTP 10-150 (Seconds): 110

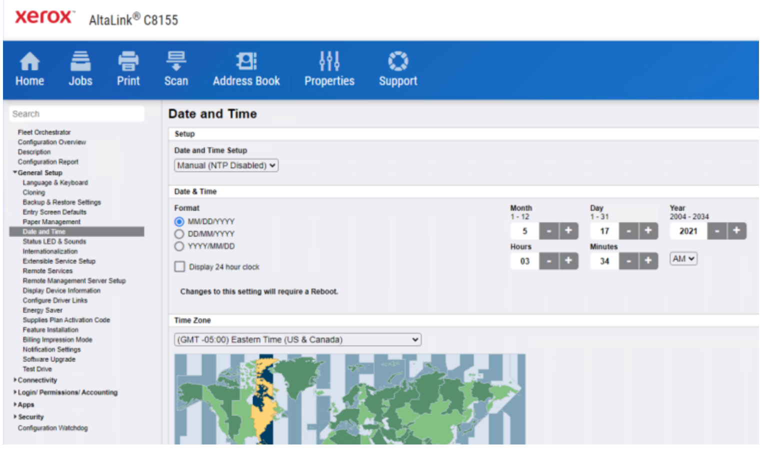
Changes to this setting will require a Reboot.

Date & Time

Format:
● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

Month 1 - 12: 10
Day 1 - 31: 20
Year 2004 - 2034: 2021
Hours: 21
Minutes: 5

    c. When not using a NTP server:
        i. Enter the correct date and time settings (must match the PaperCut MF Application Server)



Date and Time

Setup

Date and Time Setup: Manual (NTP Disabled)

Date & Time

Format:
● MM/DD/YYYY
○ DD/MM/YYYY
○ YYYY/MM/DD

☐ Display 24 hour clock

Month 1 - 12: 5
Day 1 - 31: 17
Year 2004 - 2034: 2021
Hours: 03
Minutes: 34
AM

Changes to this setting will require a Reboot.

Time Zone: (GMT -05:00) Eastern Time (US & Canada)

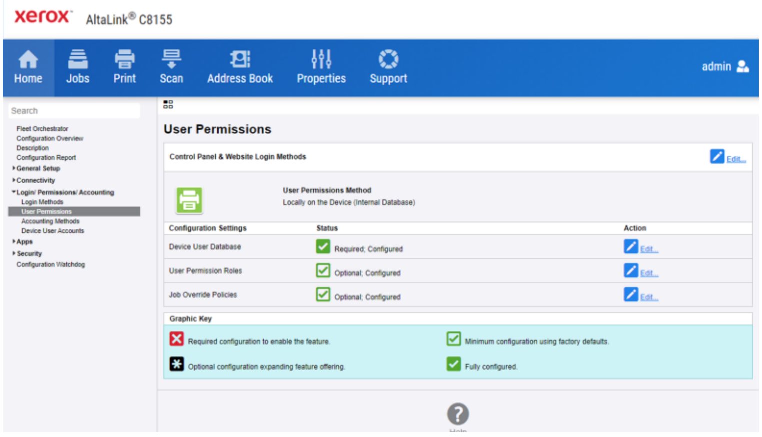
        ii. Ensure the time zone is set to the same time zone (including daylight saving) as that on the PaperCut MF Application Server.

Note: Please ensure that the device and the PaperCut MF Application Server's time settings are synchronized to within 5 minutes. Failure to do so may result in an inability to install PaperCut MF on your device.

2.8.4 Configure the device's User Permission Roles settings

To configure the device's Network Accounting settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Properties (tab) > Login/ Permissions/ Accounting > User Permissions** and select **Edit** on User Permission Roles



User Permissions

Control Panel & Website Login Methods

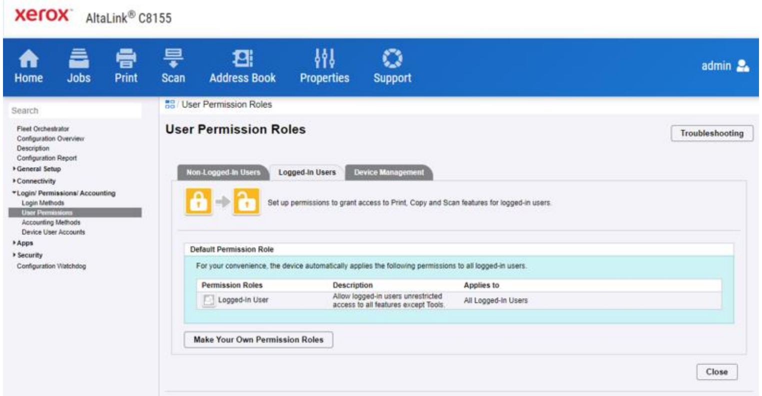
User Permissions Method
Locally on the Device (Internal Database)

Configuration Settings	Status	Action
Device User Database	✓ Required; Configured	Edit...
User Permission Roles	✓ Optional; Configured	Edit...
Job Override Policies	✓ Optional; Configured	Edit...

Graphic Key

☒ Required configuration to enable the feature.	☑ Minimum configuration using factory defaults.
✱ Optional configuration expanding feature offering.	✓ Fully configured.

3. Select the **Non-Logged-In tab** and configure the features you wish to remain active for a user that is not logged in.
4. Return to **Properties (tab) > Login/ Permissions/ Accounting > User Permissions** and select the **Logged-In Users** tab and ensure permissions for logged in users are configured as shown below (Description: "Allow logged-in users unrestricted access to all features except Tools.")



User Permission Roles

Set up permissions to grant access to Print, Copy and Scan features for logged-in users.

Default Permission Role

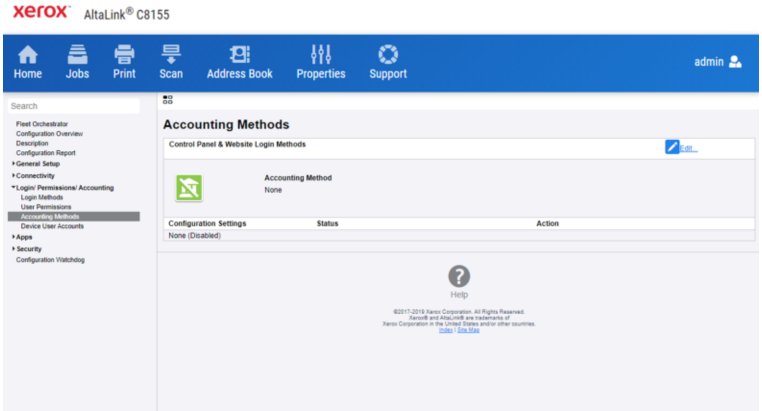
For your convenience, the device automatically applies the following permissions to all logged-in users.

Permission Roles	Description	Applies to
Logged-In User	Allow logged-in users unrestricted access to all features except Tools.	All Logged-In Users

2.8.5 Configure the device’s Network Accounting settings

To configure the device’s Network Accounting settings:

1. Log in to the device’s web interface as an administrator.
2. Navigate to **Properties (tab) > Login/ Permissions/ Accounting > Accounting Methods** and ensure that **Accounting Method** and select **Edit** on Control Panel & Website Login Methods



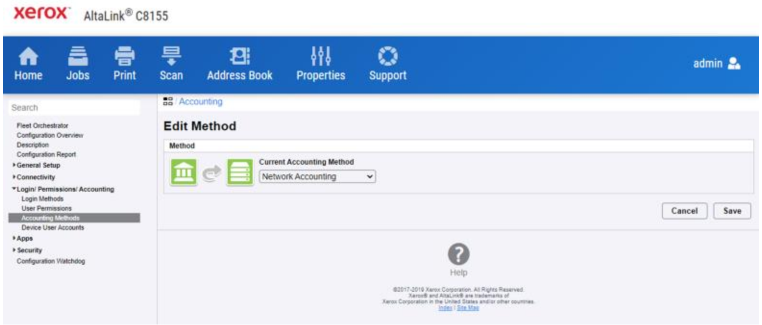
Accounting Methods

Control Panel & Website Login Methods

Accounting Method
None

Configuration Settings	Status	Action
None (Disabled)		

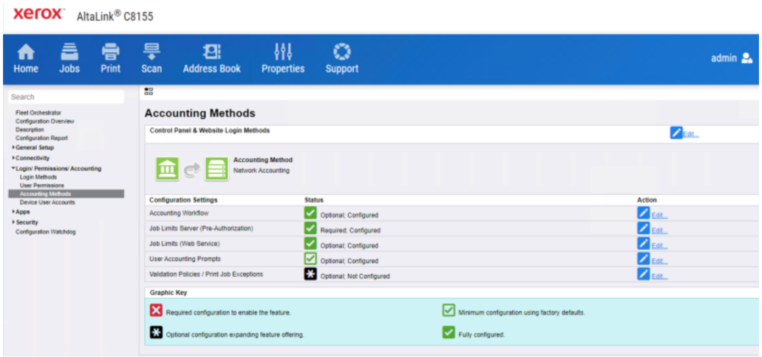
3. Set **Current Accounting Method** to **Network Accounting** and select **Save**



Edit Method

Method

Current Accounting Method: Network Accounting



Accounting Methods

Control Panel & Website Login Methods

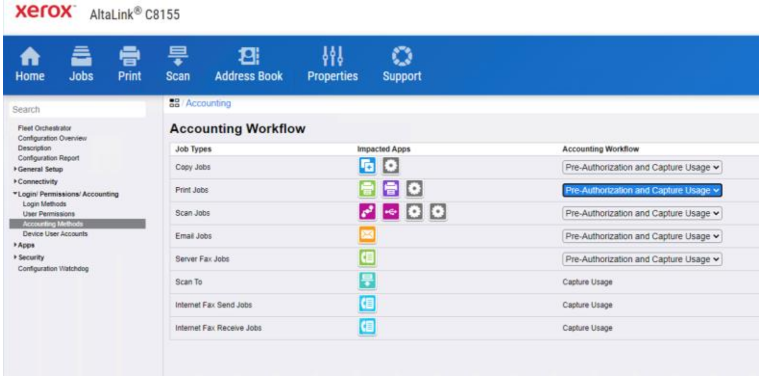
Accounting Method
Network Accounting

Configuration Settings	Status	Action
Accounting Workflow	✓ Optional; Configured	Edit...
Job Limits Server (Pre-Authorization)	✓ Required; Configured	Edit...
Job Limits (Web Service)	✓ Optional; Configured	Edit...
User Accounting Prompts	☑ Optional; Configured	Edit...
Validation Policies / Print Job Exceptions	✱ Optional; Not Configured	Edit...

Graphic Key

☒ Required configuration to enable the feature.
☑ Minimum configuration using factory defaults.
✱ Optional configuration expanding feature offering.
✓ Fully configured.

4. In **Accounting Workflow**, select **Edit, then** configure the listed workflows and select **Save** as noted below to ensure funds are available before the job is executed



Accounting Workflow

Job Types	Impacted Apps	Accounting Workflow
Copy Jobs		Pre-Authorization and Capture Usage
Print Jobs		Pre-Authorization and Capture Usage
Scan Jobs		Pre-Authorization and Capture Usage
Email Jobs		Pre-Authorization and Capture Usage
Server Fax Jobs		Pre-Authorization and Capture Usage
Scan To		Capture Usage
Internet Fax Send Jobs		Capture Usage
Internet Fax Receive Jobs		Capture Usage

2.8.6 Troubleshooting installation

2.8.6.1 Troubleshooting AltaLink 8100 series & EC8000 series Installation

It is possible that some configuration changes that are made during the registration process require a reboot of the device before registration can be completed. Should any unexpected issues be encountered during the installation process, attempt a reboot. PaperCut MF will attempt to continue registration following the device's reboot.

Additionally, check the Device Status in the PaperCut Device Settings page. If a message appears that indicates an 'IP Lockout' or 'Authentication Failure' has occurred, please ensure the date and time settings in 2.8.3 Configure the device's Date and Time settings are applied and that the correct device admin credentials have been entered into PaperCut MF.

2.8.6.2 Troubleshooting AltaLink C8145 & C8155 Installation

There have been known issues installing PaperCut MF on the AltaLink C8145 & C8155 devices with older firmware versions. If your device does not successfully register and complete integration with PaperCut MF, it is recommended that you perform a factory reset.

To obtain latest the firmware for your device, please contact your Xerox reseller or Xerox directly for further support.

3 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+)*.

- 3.2 Jobs with a simple workflow
- 3.3 Jobs with an advanced workflow

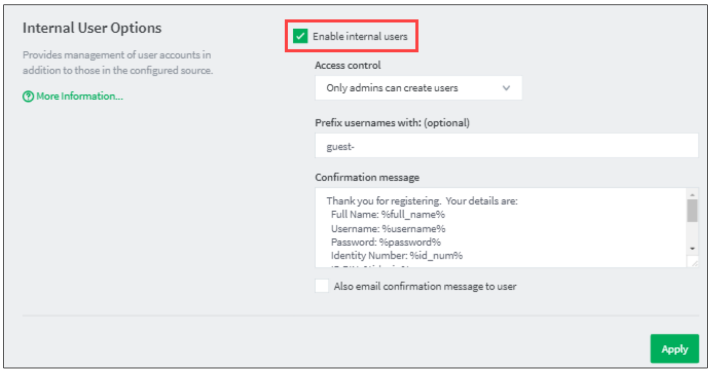
3.1 Test preparation: create test users

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

- **Simple test user** – A user who performs jobs using a simple workflow (i.e. without the task of cost allocation).
- **Advanced test user** – A user who performs jobs using an advanced workflow (i.e. with the task of cost allocation).

To create test users:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > User/Group Sync**.
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.

☑ Enable internal users

Access control: Only admins can create users

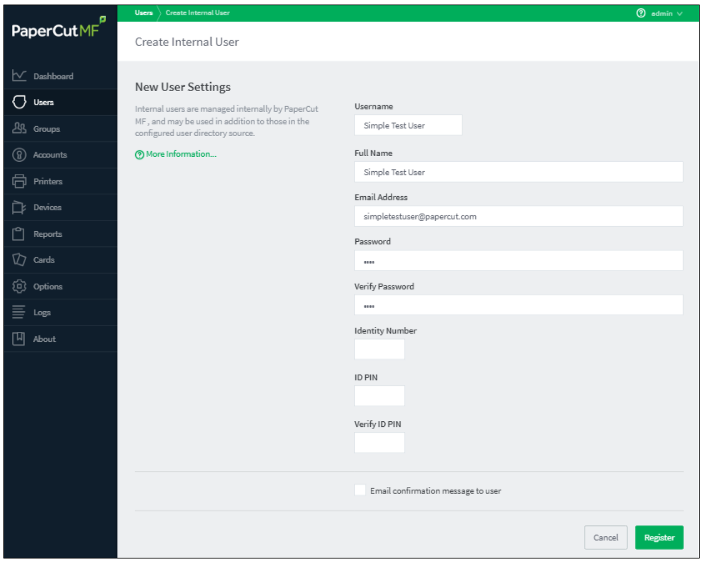
Prefix usernames with: (optional): guest-

Confirmation message:

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

☐ Also email confirmation message to user

5. Navigate to **Users**.
6. Click **Create internal user…**
7. Enter the required details for the test users as required (simple test user, advanced test user):



Create Internal User

New User Settings

Internal users are managed internally by PaperCut MF, and may be used in addition to those in the configured user directory source.

Username: Simple Test User

Full Name: Simple Test User

Email Address: simpletestuser@papercut.com

Password: ••••

Verify Password: ••••

Identity Number:

ID PIN:

Verify ID PIN:

☐ Email confirmation message to user

8. Click **Register**.

3.2 Jobs with a simple workflow

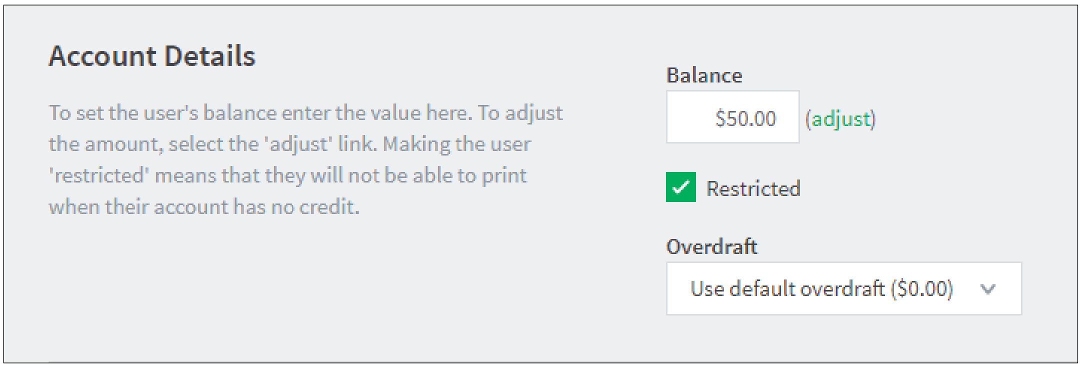
Jobs using a simple workflow are jobs that are performed without the task of cost allocation. It does not involve providing the simple test user with a choice of accounts to choose from.

3.2.1 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 3.1 Test preparation: create test users. Once created, ensure the simple test user is configured.

To configure the simple test user:

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



Account Details

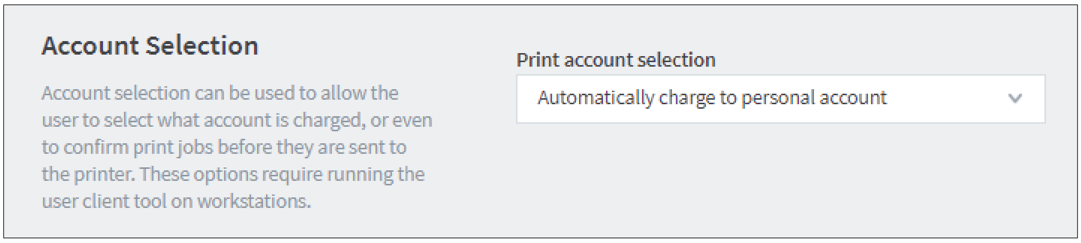
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: $50.00 (adjust)

☑ Restricted

Overdraft: Use default overdraft ($0.00)

5. 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.

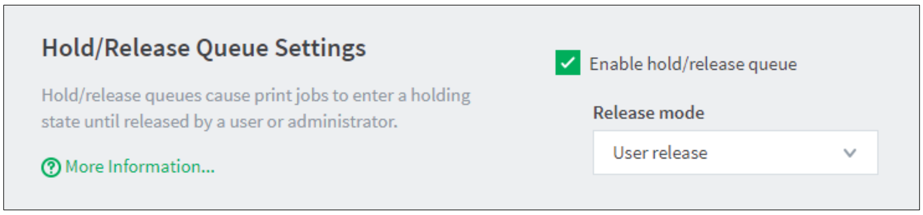
Print account selection: Automatically charge to personal account

6. Click **Apply**.

3.2.2 Simple printing

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 3.1 Test preparation: create test users and 3.2.1 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:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Printers**.
  3. Select the Printer that is applicable to the device being tested.
  4. In the **Hold/Release Queue Settings** area, select the **Enable hold/release queue**.



Hold/Release Queue Settings

Hold/release queues cause print jobs to enter a holding state until released by a user or administrator.

☑ Enable hold/release queue

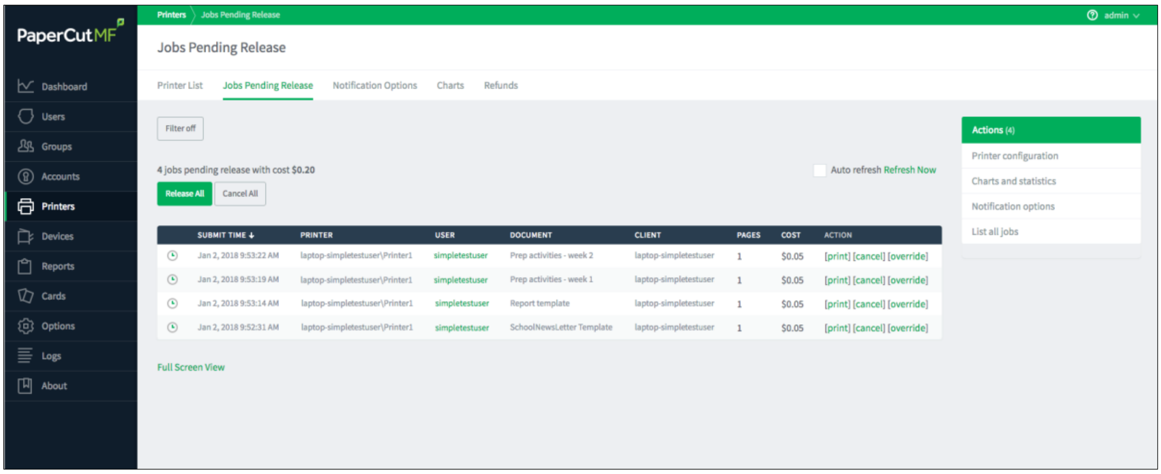
Release mode: User release

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

- **Device functions** – Printing is enabled. To enable printing:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Devices**.
  3. Select the required device being tested.
  4. In the **Print Release** area, select **Enable print release**.
  5. 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.
  6. Click **Apply**.
  7. Verify that the **Devices > External Device List** displays the device with **Print Release** in the **Function** column.

To test a simple print job:

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:



Jobs Pending Release

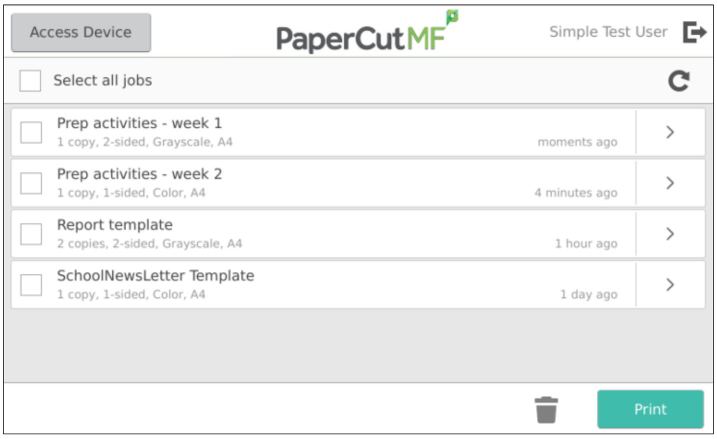
4 jobs pending release with cost $0.20

☐ Auto refresh Refresh Now

	SUBMIT TIME ↓	PRINTER	USER	DOCUMENT	CLIENT	PAGES	COST	ACTION
🕒	Jan 2, 2018 9:53:22 AM	laptop-simpletestuser\Printer1	simpletestuser	Prep activities - week 2	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
🕒	Jan 2, 2018 9:53:19 AM	laptop-simpletestuser\Printer1	simpletestuser	Prep activities - week 1	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
🕒	Jan 2, 2018 9:53:14 AM	laptop-simpletestuser\Printer1	simpletestuser	Report template	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]
🕒	Jan 2, 2018 9:52:31 AM	laptop-simpletestuser\Printer1	simpletestuser	SchoolNewsLetter Template	laptop-simpletestuser	1	$0.05	[print] [cancel] [override]

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:



☐ Select all jobs

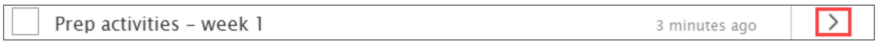
☐ Prep activities - week 1
1 copy, 2-sided, Grayscale, A4 moments ago

☐ Prep activities - week 2
1 copy, 1-sided, Color, A4 4 minutes ago

☐ Report template
2 copies, 2-sided, Grayscale, A4 1 hour ago

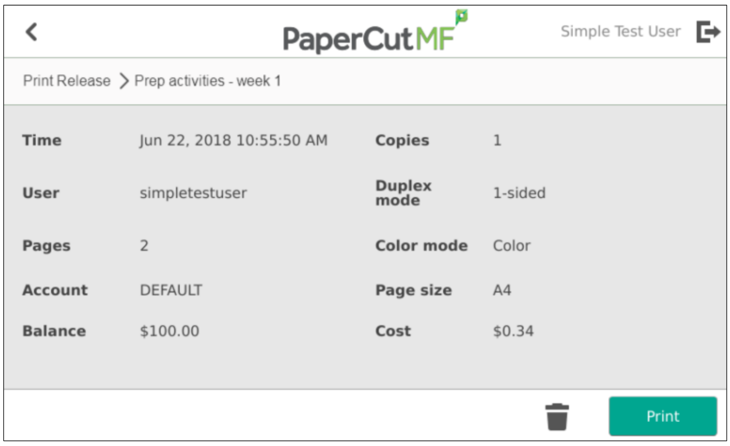
☐ SchoolNewsLetter Template
1 copy, 1-sided, Color, A4 1 day ago

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:



☐ Prep activities – week 1 3 minutes ago

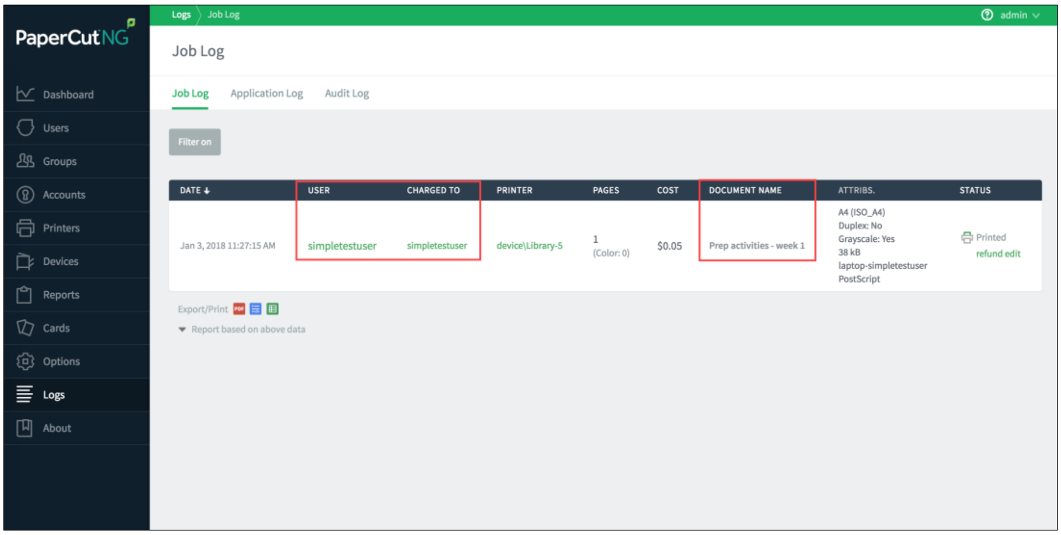
Details of the held print job are displayed:



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

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.

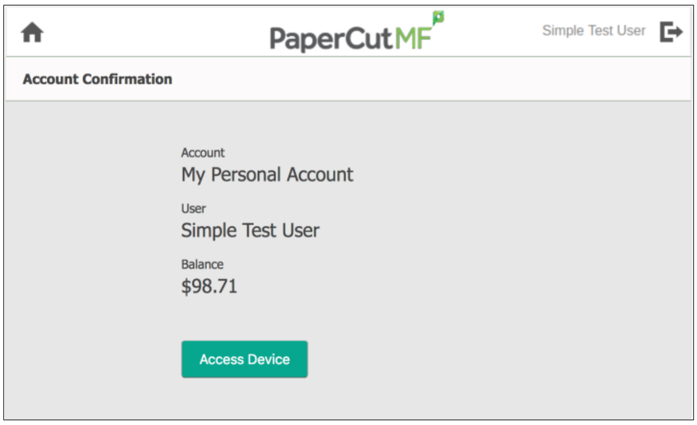
3.2.3 Simple copying or on-device printing

To test simple copying or on-device printing, ensure the following test preparation requirements are met:

- **Simple test user** - A simple test user is created and configured. For more information, see 3.1 Test preparation: create test users and 3.2.1 Test preparation: configure simple test user
- **Device functions** – Copying is enabled. To enable copying:
    1. Log in to the PaperCut MF Admin web interface.
    2. Navigate to **Devices**.
    3. Select the required 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 a simple copy or on-device print job:

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:



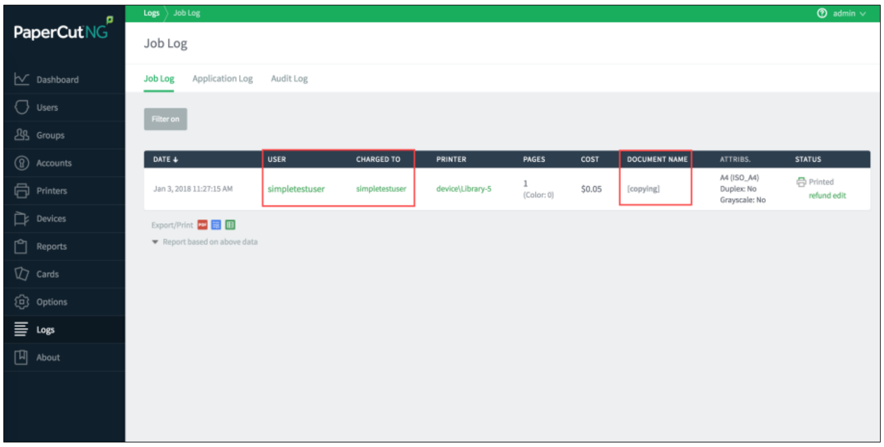
Account Confirmation

Account
My Personal Account

User
Simple Test User

Balance
$98.71

3. Complete the simple copy or on-device print job.
4. Log out of the device.
5. Log in to the PaperCut MF Admin web interface.
6. Navigate to **Logs**.
7. After the job 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	[copying]	A4 (ISO_A4) Duplex: No Grayscale: No	Printed refund edit

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

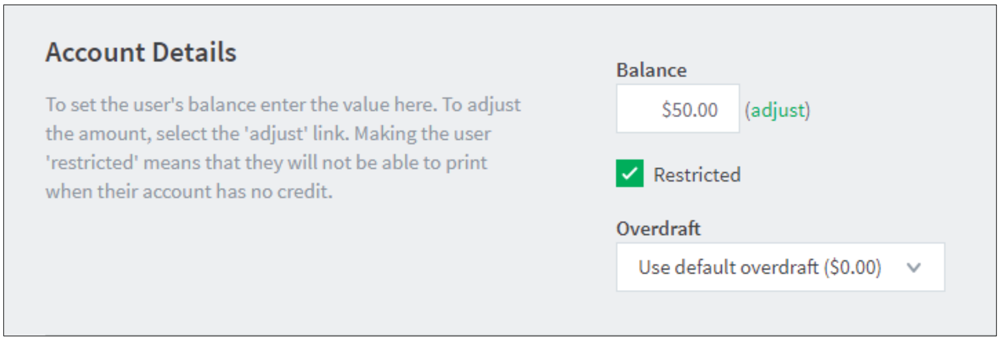
3.3 Jobs with an advanced workflow

Jobs using an advanced workflow are jobs that are performed with the task of cost allocation. It involves providing the advanced test user with a choice of accounts to choose from. The job is charged to the account that is selected by the advanced test user.

To test a job (such as, a copy job or an on-device print job) using an advanced workflow, ensure the following test preparation requirements are met:

- **Advanced test user** – An advanced test user must be created. For more information, see 3.1 Test preparation: create test users.
  Once created, the advanced test user must be configured.
  To configure the advanced test user:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Users**.
  3. From the **User List**, select the advanced test user.

4. In the **Account Details** area, set the **Balance** to **$50.00** and select **Restricted:**



Account Details

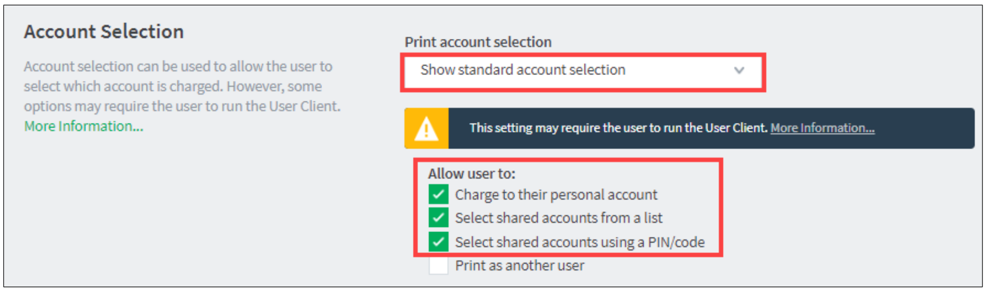
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: $50.00 (adjust)

☑ Restricted

Overdraft: Use default overdraft ($0.00)

5. In the **Account Selection** area's **Print account selection**, select **Show standard account selection** and select the required options:



Account Selection

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

Print account selection: Show standard account selection

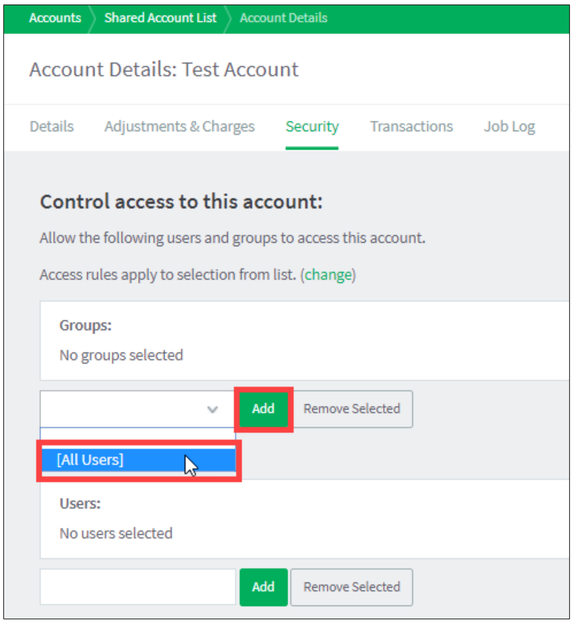
This setting may require the user to run the User Client. More Information...

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

6. Click Apply.

- **Device functions** – Copying is enabled. To enable copying:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Devices**.
  3. Select the required 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 1).
  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] and click **Add**:



Account Details: Test Account

Control access to this account:

Allow the following users and groups to access this account.

Access rules apply to selection from list. (change)

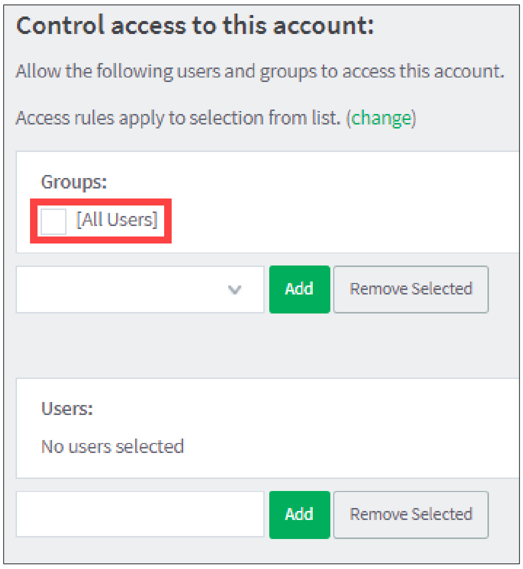
Groups:

No groups selected

Users:

No users selected

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



Control access to this account:

Allow the following users and groups to access this account.

Access rules apply to selection from list. (change)

Groups:

☐ [All Users]

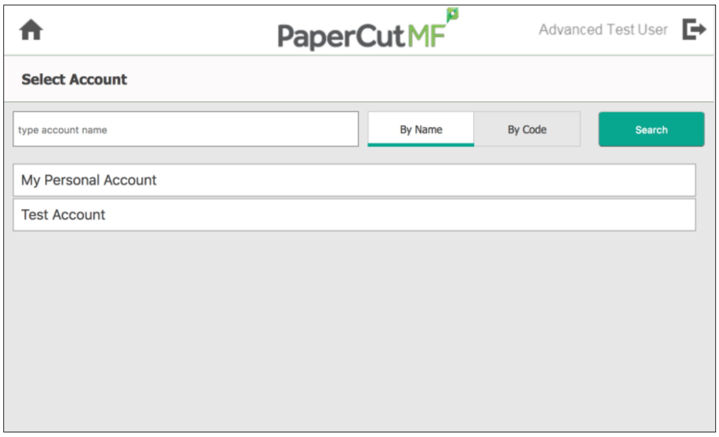
Users:

No users selected

To test a job (such as, a copy job or an on-device print job) using an advanced workflow:

1. Log in to the device as the advanced test user.

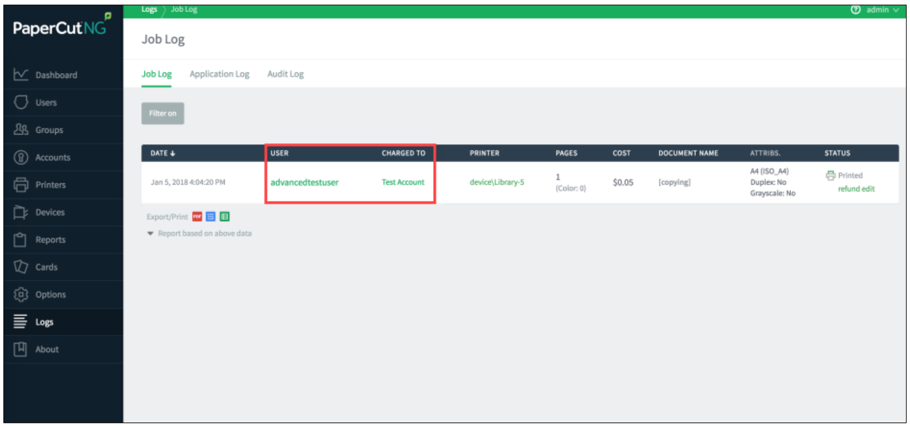
2. Verify that the PaperCut MF Select Account screen provides the advanced test user with a choice of accounts to choose from:



My Personal Account

Test Account

3. Select the required account, Test account 1.
4. Complete the job by following the device’s workflow.
5. The job is charged to the account selected by the advanced test user, Test account 1.
6. Log out of the device.
7. Log in to the PaperCut MF Admin web interface.
8. Navigate to **Logs**.
9. After the job 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:



DATE ↓	USER	CHARGED TO	PRINTER	PAGES	COST	DOCUMENT NAME	ATTRIBS.	STATUS
Jan 5, 2018 4:04:20 PM	advancedtestuser	Test Account	device\Library-5	1 (Color: 0)	$0.05	[copying]	A4 (ISO_A4) Duplex: No Grayscale: No	Printed refund edit

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

4 Configuration

PaperCut MF is installed on the device with default settings, which are reasonable for most environments. However, these settings can be further tweaked to suit your environment.

This section covers the configuration changes that can be made to the default settings of *PaperCut MF - Xerox (Secure Access EIP 1.5+)*.

4.1 Inbound connections

4.1.1 Inbound connections to PaperCut MF Application Server

To configure PaperCut MF to allow inbound connections from the device to the PaperCut MF Application Server, use the config key **system.network-address**. For more information, see 4.9 Config Editor.

4.1.2 Inbound connections to PaperCut MF Site Servers

To configure PaperCut MF to allow inbound connections from the device to PaperCut MF Site Servers:

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

4.2 Additional network security

By default, the PaperCut MF Application Server allows device connections from any network address. However, communication between the PaperCut MF Application Server and the device can be further restricted to a set range of network addresses. This provides an additional level of security and ensures that only approved devices are connected to the PaperCut MF Application Server.

To restrict communication between the PaperCut MF Application Server and the device to a subset of IP addresses or subnets:

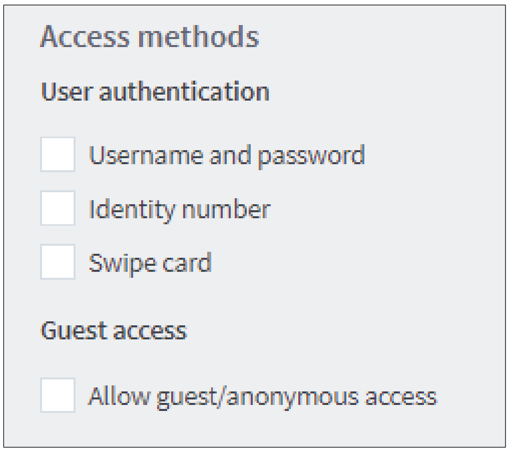
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **Security** area's field **Allowed device IP addresses**, enter a comma-separated list of device IP addresses or subnets (<ip-address1 or subnet-mask1>, <ip-address2 or subnet-mask2>).
4. Click **Apply**.

4.3 User authentication options

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

To configure the device's user authentication:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
   The available user authentication options 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

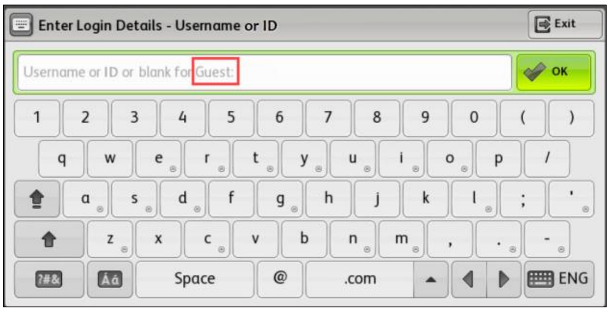
Note: You may use any one or a combination of all the available user authentication options, including the anonymous and guest access authentication.

The available user authentication options are:

User authentication option	Description
Username and password	This is the default authentication option. With this option, users use their domain/network username and password.
Identity number	With this option, users use their ID number. For more information, see the [PaperCut MF manual](#). • **Require PIN:** With this option, users use their id number and the PIN associated with the id number. **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.
Swipe card	With this option, users use their registered swipe card (e.g. magnetic strip, smart card, RFID). For more information, see the [PaperCut MF manual](#).

	Note: If you select this option, then see 4.4 User authentication via swipe cards. • **Require PIN:** With this option, users use their registered swipe card and the PIN associated with the card. **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. • **Enable self-association with existing user accounts**: With this option, users can use a registered swipe card or a new, unregistered swipe card. If 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 required, 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.** For more information, see 4.9 Config Editor.
Allow guest/anonymous access	With this option, 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. • **Guest access** - Selecting the **Allow guest/anonymous access** authentication option *and also* selecting one or more of the other authentication options (Username and password, Identity number, Swipe card), activates **Guest access**. With this option: ○ If the **Allow guest/anonymous access** authentication option is selected together with only the **Swipe card** authentication option, 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 option is selected together with any

other authentication option - **Username and password**, **Identity number -** with or without the **Swipe card** authentication option, then the user is presented with a **Guest** instruction (which you can customize using the config key **ext-device.xerox.guest-access.label**) together with instructions for all other authentication options 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.

- **Anonymous access** - Only selecting the **Allow guest/anonymous access** authentication option *without* selecting any other authentication option, activates **Anonymous access**. With this option:
    - 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.

4.4 User authentication via swipe cards

If the **Swipe card** authentication option is selected (see 4.3 User authentication options, 4.4.3 Handling card identifiers), then depending on the type of card reader being used, see:

- 4.4.1 Supported network card readers
- 4.4.2 Supported USB card readers

4.4.1 Supported network card readers

Network card readers are not physically connected to the device. The PaperCut MF Application Server communicates with these card readers over the network.

PaperCut MF - Xerox (Secure Access EIP 1.5+) supports the following configured and compatible network card readers:

- Elatec TWN3 Card Readers with the TCP Converter
- RF Ideas Ethernet Card Readers

To configure your supported network card reader:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In **External Device Settings > Access methods > User authentication**, select **Swipe Card > Enable network card reader**.
5. Enter the required details of your network card reader (**Connection Mode, Hostname/ IP, Port**).
6. Click **Apply**.

4.4.2 Supported USB card readers

USB card readers are physically connected to the device.

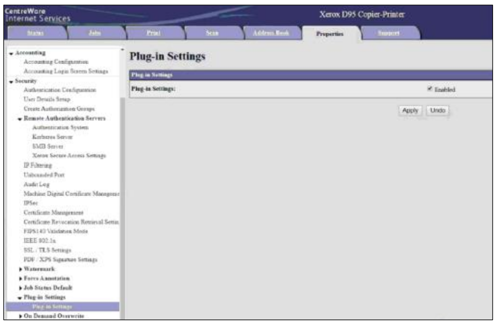
PaperCut MF - Xerox (Secure Access EIP 1.5+) supports the following configured and compatible USB card readers:

- Proximity card readers – RFIdeas, Elatec TWN3, Elatec TWN4
- Magstripe card readers – Magtek, IDTech MiniMag, RF Ideas MS3-00M1AKU
- Barcode card readers - Honeywell (3800G04), Motorola (DS9208, DS457)

To configure your supported USB card reader:

1. Depending on your Xerox device, navigate to the relevant Xerox web page that lists the USB Card Reader Plug-In file that is required for your Xerox device.
   For example, for VersaLink devices such as B405, running EIP 3.7, see *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 required USB Card Reader Plug-In zip file.
   For example, *Cardreader_plugin_with_signature.zip*
3. From the downloaded zip file, extract the required cardreader with signature JAR file.
   For example, *cardreader_sig.jar*.
4. Log in to the device’s web interface as an administrator.
5. Navigate to **System > Plug-in Settings**.
6. Ensure the **Plug-in Settings/ Plug-in Feature** is enabled.

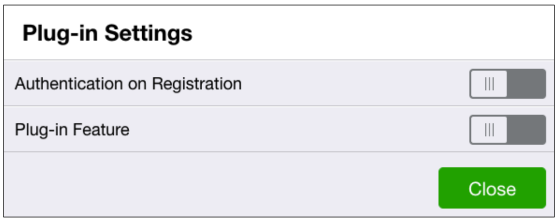
D95	B405



Plug-in Settings

Plug-in Settings

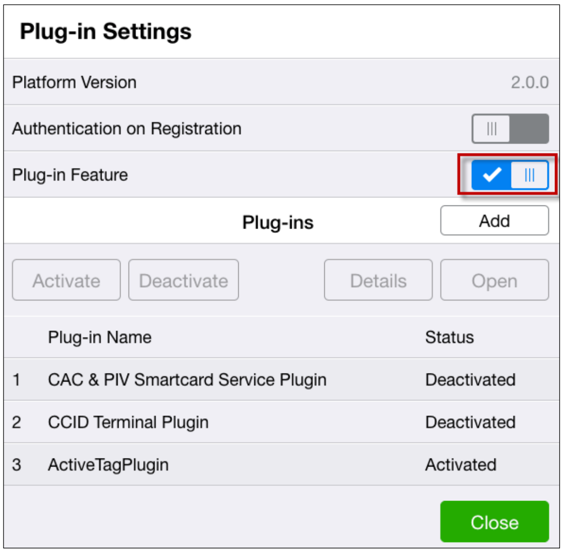
Plug-in Settings: ☑ Enabled



Plug-in Settings

Authentication on Registration ☐

Plug-in Feature ☐



Plug-in Settings

Platform Version 2.0.0

Authentication on Registration ☐

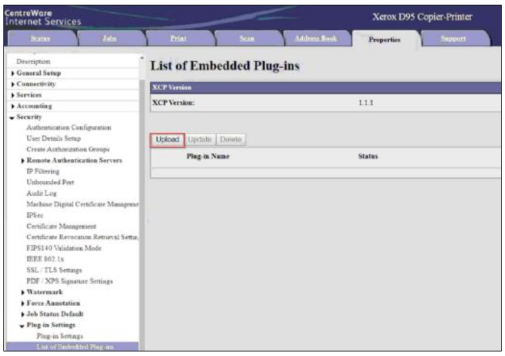
Plug-in Feature ☑

Plug-ins

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

7. Restart the device.
8. Log in to the device’s web interface as an administrator.
9. Navigate to **System > Plug-in Settings**.
10. Upload the extracted cardreader with signature JAR file. For example, *cardreader_sig.jar*.

D95	B405

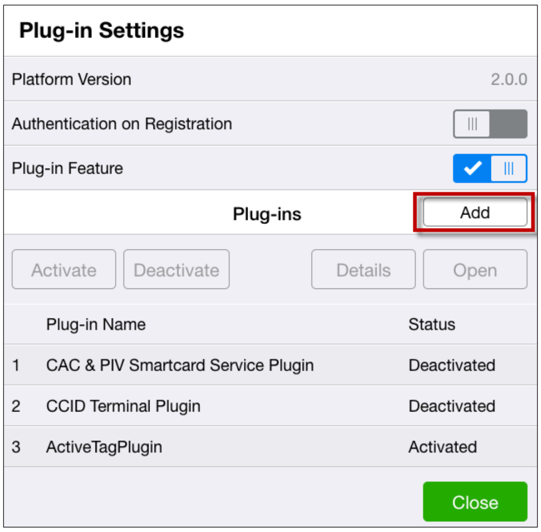


List of Embedded Plug-ins

XCP Version

XCP Version: 1.1.1

Plug-in Name	Status



Plug-in Settings

Platform Version 2.0.0

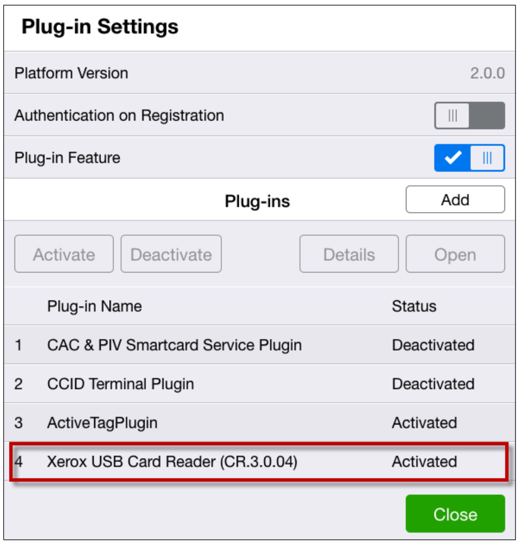
Authentication on Registration ☐

Plug-in Feature ☑

Plug-ins

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

11. Restart the device.
12. Navigate to **System > Plug-in Settings.**
13. Verify that the status of the Xerox USB Card Reader Plug-in is **Activated**.



Plug-in Settings

Platform Version 2.0.0

Authentication on Registration

Plug-in Feature ✓

	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

4.4.3 Handling card identifiers

By default, PaperCut MF handles each card's unique identifier using the following pre-configured option:

- Cards whose identifiers consist of a number followed by special character and a checksum, are modified to include only the number (the special character and everything after it is ignored). This extracted, shortened identifier is used to identify the card and the corresponding user within PaperCut MF. For example, a card with the unique identifier 5235092385=8 is modified to 5235092385.

You can also tweak the way PaperCut MF handles each card's identifier by using any of the following options:

- Using utility or configuration tools directly on the card reader's hardware.
- Using third party applications to decrypt card identifiers. For more information, contact your reseller or Authorized Solution Center.
- Using the following options within PaperCut MF:
    - Regular expression filters
    - Converters (standard format converters and custom JavaScript converters)

    Note: If you use both an expression *and* a converter, then the card's identifier is handled first by the expression and then further by the converter

  Verify the results of the expressions, convertors, or both applied using the PaperCut MF Admin web interface's **Application Log**.

4.4.3.1 Regular expression filters

To extract and validate card identifiers using regular expression filters, use the config keys **ext-device.card-no-regex, ext-device.self-association-allowed-card-regex.**

Note: If you customize BOTH the config keys **ext-device.card-no-regex** and **ext-device.self-association-allowed-card-regex**, then you must ensure that:

- **ext-device.card-no-regex** is the extraction pattern (i.e. the "full regular expression filter" based on which card identifiers are extracted)

- **ext-device.self-association-allowed-card-regex** is the validation pattern (i.e. validates only the “truncated part of the card identifier” that was extracted by the extraction pattern of **ext-device.card-no-regex**)

For example:

- *if, **ext-device.card-no-regex** = \d{6}(\d{8})*
- *then, **ext-device.self-association-allowed-card-regex** = \d{8}*

For more information, see 4.9 Config Editor.

Some regular expression filters include:

Expression	Description	Example
(.{10})	Extract the first 10 characters	AST%123456789 is modified to AST%123456
(\d{5})	Extract the first 5 numbers	AST%123456789 is modified to 12345
\d*=(\d*)=\d*	Extract only the numbers between the 2 special characters	123453=292929=1221 is modified to 123453292929 1221

For more information, see www.regular-expressions.info.

4.4.3.2 Standard format converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see 4.9 Config Editor.

Some examples of standard format converters are:

Converter	Description	Example
hex2dec	Convert a hexadecimal (base 16) encoded card identifier to the decimal format. **Note:** Hexadecimal numbers usually contain 0-9 and A-F.	946EBD28 is modified to 2490285352
dec2hex	Convert a decimal encoded card identifier to the hexadecimal format.	2490285352 is modified to 946EBD28
ascii-enc	Unpack an ASCII encoded card identifier to its encoded ASCII number.	3934364542443238 is modified to its ASCII code 946EBD28.

ascii-enc|hex2dec	First unpack an ASCII encoded card identifier to its encoded ASCII number. Then convert it to the decimal format. **Note:** Use a delimiting pipe (|) to chain or pipeline converters.

4.4.3.3 Custom JavaScript converters

To use a custom JavaScript converter:

1. Create a JavaScript file. For example:
   [install-path]/server/custom/card.js
2. Define a single JavaScript function in this file called **convert**. It must accept and return a single string. For example:
   ```
   function convert(cardNumber) {
     return cardNumber.substring(3,10).toLowerCase();
   }
   ```
3. Include a converter in the form: **javascript:custom/card.js**
4. Optionally, include a JavaScript script in the pipeline. For example:
   ascii-enc|hex2dec|javascript:custom/card.js
5. Verify the JavaScript converter from the following log:
   [install-path]/server/log/server.log
6. Use the config key **ext-device.card-no-converter** to modify card identifiers using custom JavaScript converters. For more information, see 4.9 Config Editor.

4.5 SNMP

You must configure the device and PaperCut MF to use SNMP. While the device uses SNMP for XSA authentication, PaperCut MF uses SNMP to:

- block the release of jobs to the device when it is in error,
- retrieve the device's printer toner levels

To configure the device to use SNMP, see:

- 2.4 Setup procedure for EIP/JBA Fuji-Xerox devices (EIP 1.5)
- 2.5 Setup procedure for ConnectKey 2.5 devices (EIP 3.0)
- 2.6 Setup procedure for VersaLink devices (EIP 3.7)
- 2.7 Setup procedure for AltaLink devices (EIP 4.0)

To configure PaperCut MF to use SNMP:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. In the **External Device Settings,** to enable PaperCut MF to use:
    - SNMPv1/v2c:

        a. Ensure the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox is not selected (default).
        b. 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/ Community Name (Read/Write).**
    - SNMPv3:
        a. Select the **Use SNMPv3 for Toner Retrieval and Device Error Monitoring** checkbox; and enter the following fields:
            - **Context name** – Do not enter any value.
            - **Username** – Enter **Xadmin**.
            - **Privacy password** – Enter the same value as the device web interface's **Privacy/ Encryption Password**.
            - **Authentication password** – Enter the same value as the device web interface's **Authentication Password**.
            - **Authentication protocol** – Select MD5.
            - **Privacy protocol** – Select DES
        b. ensure the value of the config keys are the same as the values on the device's web interface and on the PaperCut MF Admin web interface:
            - **ext-device.xerox.snmp-v3-auth-username**
            - **ext-device.xerox.snmp-v3-auth-password**
            - **ext-device.xerox.snmp-v3-privacy-password**
5. Click **Apply.**

4.6 Secure print release

Secure Print Release causes all print jobs to be held at the device until a user releases the job. If the device is configured with Secure Print Release, then when releasing held print jobs, users can select the following:

- the account
- the job attributes

To configure Secure Print Release:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In the **Print Release** area, select **Enable print release**.
5. In the **This device will display jobs for release from the selected source queues**, select the required Hold/Release queue. For more information, see the PaperCut MF manual.
   Note: Ensure this does not contradict the settings configured on the device's web interface. For more information, see:
    - 2.4 Setup procedure for EIP/JBA Fuji-Xerox devices (EIP 1.5)
    - 2.5 Setup procedure for ConnectKey 2.5 devices (EIP 3.0)
    - 2.6 Setup procedure for VersaLink devices (EIP 3.7)

  - ○ 2.7 Setup procedure for AltaLink devices (EIP 4.0)

4.6.1 User selection of an account

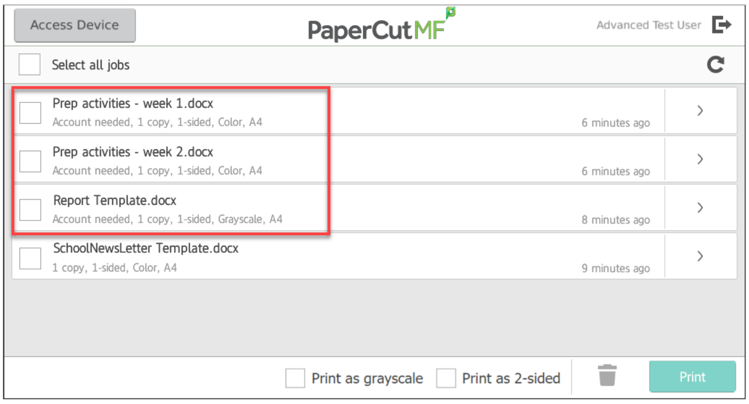
All print jobs must be allocated to an account before they can be released (printed). This account can be either:

- a user's personal account, or
- a shared account for cost center, faculty, or client billing purposes.

Users can allocate an account to a print job via the User Client and/or at the device. For more information about configuring cost allocation for users, see the PaperCut MF manual.

At the device, users can:

- allocate the same account to *multiple* held print jobs without an account:



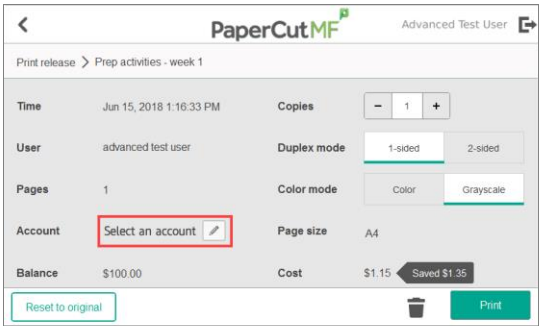
☐ Prep activities - week 1.docx
Account needed, 1 copy, 1-sided, Color, A4 — 6 minutes ago

☐ Prep activities - week 2.docx
Account needed, 1 copy, 1-sided, Color, A4 — 6 minutes ago

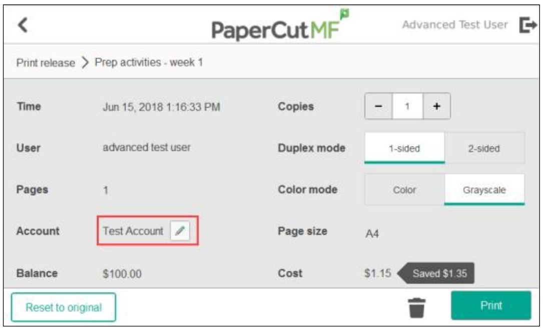
☐ Report Template.docx
Account needed, 1 copy, 1-sided, Grayscale, A4 — 8 minutes ago

☐ SchoolNewsLetter Template.docx
1 copy, 1-sided, Color, A4 — 9 minutes ago

- allocate an account to a *single* held print job without an account or change a previously allocated account:



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



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

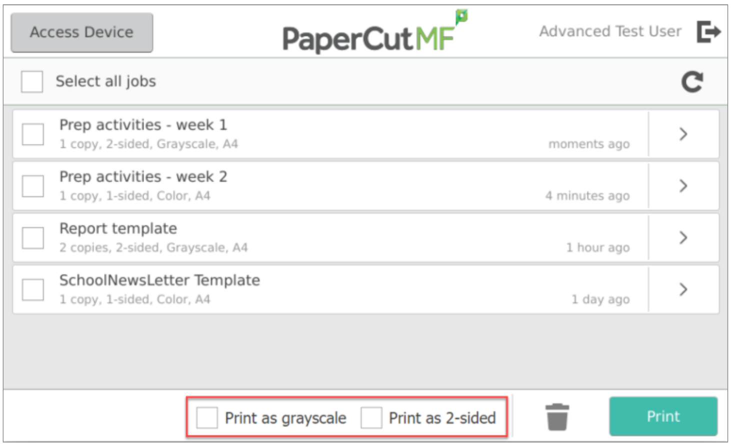
Note: By default, PaperCut MF allows users to select accounts at the device. However, you also have the option of disabling this. For more information, see the PaperCut MF manual.

4.6.2 User selection of job attributes

PaperCut MF allows users to change the attributes of held print jobs at the device, before releasing (printing) them. 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 one or many jobs, simultaneously:

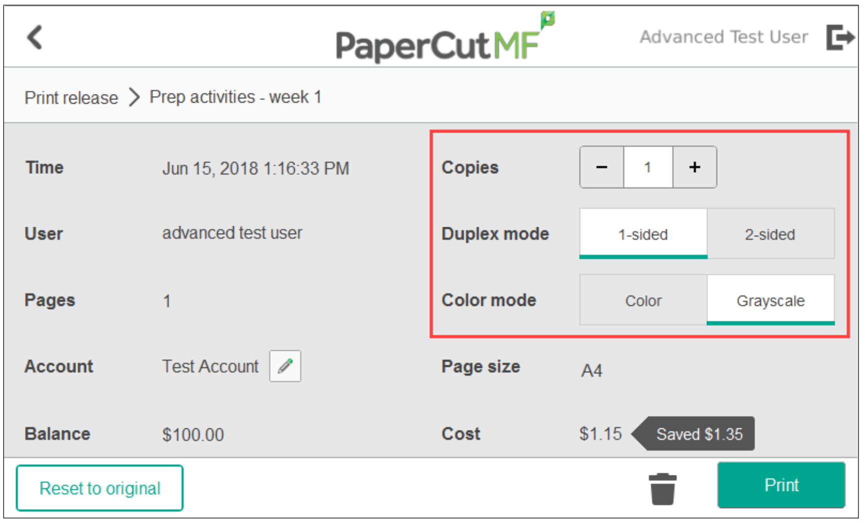
- **Print as grayscale** (from color to grayscale)
- **Print as 2-sided** (from 1-sided to 2-sided)



☐ Prep activities - week 1 — 1 copy, 2-sided, Grayscale, A4 — moments ago
☐ Prep activities - week 2 — 1 copy, 1-sided, Color, A4 — 4 minutes ago
☐ Report template — 2 copies, 2-sided, Grayscale, A4 — 1 hour ago
☐ SchoolNewsLetter Template — 1 copy, 1-sided, Color, A4 — 1 day ago

Clicking the arrow to the right of a single held print job displays all the attributes for that job, allowing users to make the following additional changes:

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



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 | 2-sided
Color mode: Color | Grayscale
Page size: A4
Cost: $1.15 Saved $1.35

To toggle the display of the cost of held print jobs on the PaperCut MF Print Release and Print Settings screens on the device, use the config key **ext-device.xerox.release-show-cost**. For more information, see 4.9 Config Editor.

Note: By default, PaperCut MF allows users to select jobs attributes at the device. However, you also have the option of disabling this. For more information, see the PaperCut MF manual.

4.7 Device jobs

Device jobs include jobs initiated at the device, such as, scan, copy, fax, on-device printing.

4.7.1 Tracking device jobs

To specify the device jobs that PaperCut MF tracks and controls:

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

4. In the **External Device Settings** area, select the required device jobs:
    - **Track & control copying** – PaperCut MF tracks and controls copy jobs and on-device print jobs
    - **Track & control scanning** – PaperCut MF tracks and controls scan jobs
      Note: This is only applicable to multi-function devices.
    - **Track & control faxing** – PaperCut MF tracks and controls fax jobs
      Note: This is only applicable to multi-function devices.

   Note: Ensure this does not contradict the settings configured on the device's web interface. For more information, see:
    - ○ 2.4 Setup procedure for EIP/JBA Fuji-Xerox devices (EIP 1.5)
    - ○ 2.5 Setup procedure for ConnectKey 2.5 devices (EIP 3.0)
    - ○ 2.6 Setup procedure for VersaLink devices (EIP 3.7)
    - ○ 2.7 Setup procedure for AltaLink devices (EIP 4.0)

4.7.2 User selection of an account

If tracked device jobs (scan, copy, fax, on-device printing) are also being charged, then users must allocate them to an account.

This account can be either:

- a user's personal account, or
- a shared account for cost center, faculty, or client billing purposes.

The options available to users at the device, is based on the way users and the device are configured:

- For more information about configuring cost allocation for users, see the PaperCut MF manual.
- To toggle the display of the PaperCut MF Account Confirmation screen, use the **Show account confirmation** checkbox on the PaperCut MF Admin web interface (**Devices Details > Summary > External Device Settings > Device Options**).
- To configure the PaperCut MF Select Account screen, use the config key **ext-device.xerox.initial-account-tab.** For more information, see 4.9 Config Editor.

4.7.3 Job costs and account balances (Zero Stop)

When printing, if a restricted user's account balance is insufficient to cover the cost of the restricted user's entire print job, PaperCut MF prevents the user from being able to start the print job. This ensures that the restricted user's account balance never drops below zero for print jobs.

When scanning or copying, PaperCut MF calculates the cost of a single page (i.e. the Reference Page Cost, which is based on configured values). Using this Reference Page Cost, PaperCut MF calculates the number of reference pages that the restricted user's account balance will allow (i.e. the maximum number of Reference Pages Allowed). As a result:

- If restricted user's account balance is insufficient for even one Reference Page Allowed, then PaperCut MF prevents the user from being able to start a scan or copy job.

- If restricted user's account balance is sufficient for at least one Reference Page Allowed, then PaperCut MF allows the user to start a scan or copy job.
  As the job is in progress, if the maximum number of Reference Pages Allowed is reached, then PaperCut MF:
    - stops the job,
    - prevents it from being completed, and
    - deletes the job from the device's Job Status screen.

This ensures that the restricted user's account balance never drops below zero for scan or copy jobs. For more information, see 4.7.3.1 Reference Page Cost and maximum number of Reference Pages Allowed.

4.7.3.1 Reference Page Cost and maximum number of Reference Pages Allowed

To configure the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for copy and scan jobs, use the following config keys:

- **ext-device.xerox.limit-reference.duplex**
- **ext-device.xerox.limit-reference.paper-size**

For more information, see 4.9 Config Editor

Note: This Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for copy and scan jobs have some limitations. For more information, see 5 Known Limitations and Security.

4.7.4 PaperCut MF's Integrated Scanning

Note: This is only applicable to multi-function devices that are running the latest version of EIP 3.0 or above.

To enable users to use PaperCut MF's Integrated Scanning:

1. Configure it on the PaperCut MF Admin web interface.
   For more information, see Integrated Scanning or the PaperCut MF manual.
2. Depending on the needs of your environment, you may need to change the default settings of the following config keys:
    - **ext-device.xerox.track-scan-to-ifax-as-fax-jobs**
    - **ext-device.xerox.integrated-scan-job-compression**
    - **ext-device.xerox.scan.prompt.checkbox.checked**
    - **ext-device.xerox.timeout.scan-prompt-send.secs**
    - **ext-device.xerox.timeout.complete-scan-job.secs**

   For more information, see 4.7.4.1 Integrated scan workflow, 4.9 Config Editor.
3. Ensure that the device is configured as required:
    a. Log in to the device's web interface as an administrator.
    b. Navigate to **Services > Workflow Scanning > General Settings**.
    c. In **Confirmation Sheet**, select **Off.**
       Note: This prevents the device from printing a device report for cancelled scan jobs.

4.7.4.1 Integrated scan workflow

If Integrated Scanning is enabled, then you can use the config key **ext-device.xerox.scan.prompt.checkbox.checked** to specify whether the **Prompt for more pages** checkbox on the Scan Details screen and the Scan Settings screen, is checked or unchecked by default (See 4.9 Config Editor):

- A checked **Prompt for more pages** checkbox enables the device to display the Scan More or Finish screen, providing users with the ability to add more pages to the current scan job or start new scan jobs retaining the current scan job's settings and account selection attributes.
  Note: To specify the user inactivity timeout on this screen, use the config key **ext-device.xerox.timeout.scan-prompt-send.secs.** For more information, see 4.9 Config Editor.
- An unchecked **Prompt for more pages** checkbox enables the device to complete the current scan and send it to the user (scan transfer).
  Note: To specify the user inactivity timeout on this screen, use the config key **ext-device.xerox.timeout.complete-scan-job.secs**. For more information, see 4.9 Config Editor.

4.8 Screen headers

Note: This is only applicable to devices that are running the latest version of EIP 3.0 or above.

4.8.1 Header colors

To customize the colors (background and text) of the headers on all PaperCut MF screens:

1. Use the following config keys:
   ext-device.xerox.header.color
   ext-device.xerox.header.textcolor
   For more information, see 4.9 Config Editor.
2. Log in to the device as a test user (simple test user).
3. Verify that the device's header background and text colors are as required.

4.8.2 Header logo

To customize the logo on the headers of all PaperCut MF screens:

1. Create the device's header logo as per the following specifications:
   - Image height = no more than 55 pixels
   - Image width = no more than 360 pixels
   - Image file size = less than 24bit
   - Image file format = `.png`
   - Image filename = `logo.png`
   - Image file location = `[PaperCut Install Location]\server\custom\web\device\xerox\1.5\`
2. Log in to the device as a test user (simple test user).
3. Verify that the device's header logo is as required.

4.9 Config Editor

PaperCut MF provides you with several global and device-specific config keys that you can modify to suit your environment. While some keys are *only* global (impacting PaperCut MF on all devices) or *only* device-specific (impacting PaperCut MF on the selected device), other keys are *both* global *and* device-specific simultaneously. Such keys initially inherit their global settings (GLOBAL) as their default settings. However, changes made at the device-level overrides these globally inherited default settings.

To configure the device using the available global config keys (impact PaperCut MF on all devices):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Actions > Config editor (advanced).**
   Note: For more information, see the PaperCut MF manual.

To configure the device using the available device-specific config keys (impact PaperCut MF on the selected device):

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Select the required device.
4. Click **Advanced Config.**

The available config keys are:

Config name	Description
Device screens	
ext-device.xerox.locale-override	Specify a language tag adhere to the supported locale list to force the locale setting for use on the device. The locale is determined by the following priority sequence: 1. ext-device.xerox.locale-override setting 2. The language set on the Xerox device 3. 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.header.color	Customize the background color of headers on all PaperCut MF screens. This is a device-specific config key.

	• Values: Valid CSS color specifications (color names or HTML RGB, HEX #rrggbb, HSL, RGBA, HSLA values), DEFAULT • Default: DEFAULT (#fbfafa / dark green) **Note:** For more information, see 4.8.1 Header colors.
ext-device.xerox.header.textcolor	Customize the text color of headers on all PaperCut MF screens. This is a device-specific config key. • Values: Valid CSS color specifications (color names or HTML RGB, HEX #rrggbb, HSL, RGBA, HSLA values), DEFAULT • Default: DEFAULT (#888888 / white) **Note:** For more information, see 4.8.1 Header colors.
ext-device.xerox.login-instruction	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. This is a device-specific config key. Values: Any text, DEFAULT, DONOTSET (text specified in the device's web interface) Default: DEFAULT (device-specific PaperCut MF text based on Authentication methods selected) **Note:** To add a line break, use \n. For example, PaperCut Software\nSwipe your card to log in. **IMPORTANT:** It is recommended that you use only ASCII characters because of the limited support for non-ASCII characters.
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.

ext-device.xerox.force-widget-keyboard	Configure which type of keyboard is to be used - Xerox native device keyboard or Xerox widget keyboard. **Note:** This setting is only available for Xerox devices with the firmware EIP 3.0 or higher. Values: Y, N Default: N Setting this to N, uses the Xerox native device keyboard. Setting this to Y, uses the Xerox widget keyboard.
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.xerox.support-switch-mode	This is only applicable to multi-function devices.

	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.show-release-on-login	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. **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). Values: Y, N Default: Y Setting this to Y – makes PaperCut MF the default application after login, and displays the Print Release screen. 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.
ext-device.xerox.skip-release-screen-when-no-jobs	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. Values: Y, N Default: Y **Note:**

	• Setting this to Y, suppresses the PaperCut MF Home screen. Any one of the following screens is displayed, based on other settings: o The PaperCut Select Account screen OR o The PaperCut Account Confirmation screen OR o the native device functions screen This is recommended only if the device is used more for copying rather than printing. • Setting this to N, displays the PaperCut MF Home screen. This is recommended if the device is used for all functions (printing, scanning, copying).
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.welcome-text	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. Default: DEFAULT (Welcome, <username>). **Note:** This setting is overridden by the ext-device.home-screen.show-balance setting for users who have an auto-chargeable account.
ext-device.home-screen.show-balance	Configure the PaperCut Home screen to display the following based on the type of user (restricted or unrestricted): • 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 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):

	• Automatically charge to personal account OR • Automatically charge to a single shared account This key can set in Options > Config editor (advanced). Values: Y, N, Default Default: DEFAULT (N) Setting this to Y displays the auto-chargeable account and balance, based on the type of user (restricted or unrestricted). **Note:** This overrides the ext-device.xerox.welcome-text config key. **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.
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.release-app-label	Customize the text of the **PaperCut MF Print Release** icon that appears on the device. This is a device-specific config key. • Values: Any text, DEFAULT • Default: DEFAULT (Home) **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.**
ext-device.xerox.access-device.label	This is only applicable to multi-function devices. Customize the text of the **Access Device** icon that appears on PaperCut MF screens. This is a device-specific config key.

	• Values: Any text, DEFAULT • Default: DEFAULT (Access Device)
ext-device.xerox.select-account-on-login	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. **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.select-account	Specify whether to support the Account Selection app on the MFP and display of the Account Selection Page. Values: Y, N. Default: Y 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. **On EIP 3.0+ devices:** This key is not used anymore, as there is a single app registered on the MFP called “PaperCut MF”
ext-device.xerox.require-account-selection	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. 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. If set to Y, then the user must choose an account otherwise they won’t be able to perform a job.

ext-device.xerox.initial-account-tab	Customize which of the two tabs is open by default on the PaperCut MF Select Account screen. This is a device-specific config key. Values: List (default open tab is **By Name**), Code (default open tab is **By Code**) Default: List
ext-device.xerox.release-show-cost	Toggle the display of the cost of held print jobs on the PaperCut MF Print Release screens on the device. This is a device-specific config key. • Values: Y, N • Default: Y **Note:** Setting this to N – • hides the account balance, and • does not display the savings based on other changes made to held print job settings. For more information, see 4.6.2 User selection of job attributes.
ext-device.xerox.track-scan-to-ifax-as-fax-jobs	This is only applicable to multi-function devices that are running the latest version of EIP 3.0 or above. Specify whether PaperCut MF tracks and logs the device's scan-to-ifax jobs as: • scan jobs, or • fax jobs This is a device-specific config key. • Values: Y (fax jobs), N (scan jobs), DEFAULT • Default: DEFAULT (N)
ext-device.xerox.fax-to-email-user-override	This is only applicable to multi-function devices that support Fax Forward functionality. Specify whether PaperCut MF tracks fax forward jobs (as scan jobs) or ignores them since they are **incoming** fax jobs which we typically don't track.

	By default these fax forward jobs will be ignored. If the config value is set to a non-empty string then it will be used as a username to track the jobs to. This is a device-specific config key. - Values: Empty, Username (doesn’t need to be a pre-existing user). - Default: Empty (“”)
ext-device.xerox.integrated-scan-job-compression	This is only applicable to multi-function devices that are running the latest version of EIP 4.0 or above. Specify the compression level that PaperCut MF applies, when using Integrated Scanning. This is a device-specific config key. - Values: HIGH, MEDIUM, LOW, NONE - Default: MEDIUM **Note:** Setting this to NONE – - applies no compression on PDFs - applies MEDIUM compression on JPG and TIFF files
ext-device.xerox.scan.prompt.checkbox.checked	This is only applicable to multi-function devices that are running the latest version of EIP 3.0 or above. Specify 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 screen (with the three buttons – **Scan next page, Scan new document, Finish**). 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:** For more information, see 4.7.4.1 Integrated scan workflow.

"Swipe card" authentication option	
ext-device.xerox.card.magstripe-track-no	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. Default: 2 (by default only look at the data associated with track 2)
ext-device.card-self-association.use-secondary-card-number	Specify the use of the primary or the secondary card number slot to save card identifiers during card self-association. This is a global and device-specific config key. Device-specific: • Values: Y, N, GLOBAL (inherited from global settings) • Default: GLOBAL (inherited from global settings) Global: • Values: N (Primary), Y (Secondary) • Default: N **Note:** This is only applicable if the **Swipe card** - **Enable self-association with existing user accounts** authentication option is selected. For more information, see
ext-device.card-no-regex	Specify the regular expression filter to be used to extract card identifiers for authentication. This is a global and device-specific config key. Device-specific: • Values: Any valid regular expression, GLOBAL (inherited from global settings) • Default: GLOBAL (inherited from global settings)

	Global: - Values: Any valid regular expression **Note:** - This is only applicable if the **Swipe card** authentication option is selected. For more information, see 4.3 User authentication options and 4.4.3 Handling card identifiers. - Changing the default value of this config key requires you to ensure that the value of the config key **ext-device.self-association-allowed-card-regex** is only the “extracted, truncated part of the card identifier” of this config key. For example, if the config key **ext-device.card-no-regex** = *\d{6}(\d{8}),* then the config key **ext-device.self-association-allowed-card-regex** = *\d{8}.* For more information, see 4.4.3.1 Regular expression filters.
ext-device.self-association-allowed-card-regex	Specify the regular expression filter to be used to validate card identifiers during card self-association. This is a device-specific config key. - Values: Any valid regular expression, **.*** - Default: **.*** **Note:** - This is only applicable if the **Swipe card** - **Enable self-association with existing user accounts** authentication option is selected. For more information, see 4.3 User authentication options and 4.4.3 Handling card identifiers. - Changing the default value of the config key **ext-device.card-no-regex** (extracting card identifiers using customized regular expression filters) requires you to ensure that the value of this config key is only the “truncated part of the card identifier” that was extracted by the extraction pattern of **ext-device.card-no-regex**. For example, if the config key **ext-device.card-no-regex** = *\d{6}(\d{8}),* then the config key **ext-device.self-association-allowed-card-regex** =

	\d{8}. For more information, see 4.4.3.1 Regular expression filters.
ext-device.xerox.swipe-to-logout	Specify whether swiping a card when a user is logged in will log them out or be ignored. Values: Y, N. Default: Y. 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.
Job costs and account balances (Zero Stop)	
ext-device.xerox.limit-reference.duplex	This is only applicable to devices that are running the latest version of EIP 2.0 or above. When configuring the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for copy and scan jobs, specify whether the Reference Page used is a simplex page or a duplex page. This is a device-specific config key. • Values: N (simplex), Y (duplex) • Default: N **Note:** For more information, see 4.7.3.1 Reference Page Cost and maximum number of Reference Pages Allowed.
ext-device.xerox.limit-reference.paper-size	This is only applicable to devices that are running the latest version of EIP 2.0 or above. When configuring the Reference Page Cost that is used to calculate the maximum number of Reference Pages Allowed for copy and scan jobs, specify the paper size of the Reference Page used. This is a device-specific config key. • Values: Any valid paper size, DEFAULT • Default: DEFAULT (Worldwide: A4; North America: Letter) **Note:** For more information, see 4.7.3.1 Reference Page Cost and maximum number of Reference Pages Allowed.

ext-device.xerox.fallback-to-current-account	When Job Limits is enabled, customize the way PaperCut MF handles the charging of device jobs that require an account but do not have an account to charge to: PaperCut MF either prevents the job starting or charges the job to the account most recently selected or used. -IF Y = job is charged to last used/ selected account -IF N = job is failed/ denied
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.enable-usb-print	Toggle USB printing. Values: Y, N Default: Y Setting this to Y, enables USB printing when either of the following conditions are also met: • 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 Setting this to N, disables USB printing.
Network resilience, security, debug logs, uninstallation	
ext-device.xerox.enable-preauth	**Relevant to EIP 2.0+ devices only.**

	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. 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.
ext-device.xerox.configure-preauth-and-prompts	**Relevant to EIP 2.0+ devices only.** Specify whether PaperCut should configure the Accounting Workflow and Prompts on the device for full PaperCut functionality. Values: Y, N. Default: Y. 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).
ext-device.xerox.auth-user-prefix	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. 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. 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.
ext-device.xerox.enable-secure-access	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. Values: Y, N Default: Y (automatically enable Secure Access)

ext-device.xerox.lock-device	Configure PaperCut to honor or automatically re-set the device-level user authentication permissions. **Note:** Avoid modifying this setting for VersaLink devices. Values: Y, N. Default: Y Setting this to 'N' will honor device-level user authentication permissions and not automatically reset them. Setting this to 'Y' will automatically re-set device-level user authentication permissions and will require user authentication for all device functions.
ext-device.xerox.send-users-email-address-to-device	This is only applicable to multi-function devices. Specify whether or not the user's PaperCut MF email address is sent to the device on login. Values: Y, N. Default: Y. 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.
ext-device.xerox.use-job-owner	Specify the source of the user Id used to identify the owner of a job from the Xerox Job Logs: • **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.job-download-after-login-period-secs	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. Default: DEFAULT (which allows PaperCut to choose the most appropriate time – usually 10 seconds).
ext-device.xerox.always-use-ip-address-for-secure-access	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. Values: Y, N. Default: Y It is recommended that this is not modified.

ext-device.xerox.use-ssl-for-apps	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). Values: Y, N. Default: DEFAULT (N) Non-secure setting of N maybe required when looking at packet captures for diagnosing issues involved with using these apps. 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.
ext-device.block-release-on-error.snmp-error-list	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** Values: Any one or a comma-separated combination of the above error types. Default: DEFAULT (**noPaper, doorOpen, jammed, offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull**) **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**.
ext-device.block-release-on-error.snmp-byte-order-mode	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. Values: FORWARD, REVERSE, DEFAULT Default: DEFAULT (FORWARD) 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. **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. 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.
ext-device.xerox.snmpv2.set-community-name	If the SNMP configuration is SNMPv1/v2c, then specify the device web interface’s **SET Community Name.** This is a device-specific config key. • Values: same as device web interface’s **SET Community Name**, private • Default: private For more information, see 4.5 SNMP
ext-device.xerox.snmp-v3-auth-username	If the SNMP configuration is SNMPv3, then specify 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 4.5 SNMP
ext-device.xerox.snmp-v3-auth-password	If the SNMP configuration is SNMPv3, then specify 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 **Authentication password.** For more information, see 4.5 SNMP
ext-device.xerox.snmp-v3-privacy-password	If the SNMP configuration is SNMPv3, then specify 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 **Privacy password.** For more information, see
Timeouts	
ext-device.xerox.account-cache-timeout-mins	**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 **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.
ext-device.inactivity-timeout-secs	**PaperCut MF timeout**: Specify the interval of time (seconds) after which a user who is detected as being idle on PaperCut MF is automatically logged out. This is a device-specific config key. - Values: Any positive number (seconds) - Default: 60 (seconds)
ext-device.xerox.timeout.scan-prompt-send.secs	This is only applicable to multi-function devices that are running the latest version of EIP 3.0 or above. **PaperCut MF Scan More or Finish timeout:** Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan More or Finish screen (with the three buttons – **Scan next page, Scan new document, Finish**) is automatically taken to the PaperCut MF Scan Complete screen (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. This is a device-specific config key. - Values: 1-300 (seconds) - Default: 30 (seconds) **Note:** This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout. For more information, see 4.7.4.1 Integrated scan workflow.

ext-device.xerox.timeout.complete-scan-job.secs	This is only applicable to multi-function devices that are running the latest version of EIP 3.0 or above. **PaperCut MF Scan Complete timeout:** Specify the interval of time (seconds) after which a user who is detected as being idle on the PaperCut MF Scan Complete screen (with scan completed or failed status), is automatically logged out. This is a device-specific config key. • Values: 1-300 (seconds) • Default: 5 (seconds) **Note:** This timeout temporarily deactivates the PaperCut MF timeout (**ext-device.inactivity-timeout-secs**) and the device timeout. For more information, see 4.7.4.1 Integrated scan workflow.

5 Known Limitations and Security

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

5.1 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

5.1.1 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 5, 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.

5.1.2 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. **Note**: On **VersaLink** devices, the device requires a restart for the USB print setting to take effect.

5.1.3 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"

5.1.4 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 ensure that the user is not configured with the following account selection options (which allow them to select a shared account to charge to):

1. Account Selection > Print account selection > Show standard account selection >
    - Allow user to: > Select shared accounts
    - When shared account is selected > Charge shared account

2. Account Selection > Print account selection > Show advanced account selection > When shared account is selected > Charge shared account
3. Account Selection > Print account selection > Show manager mode

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

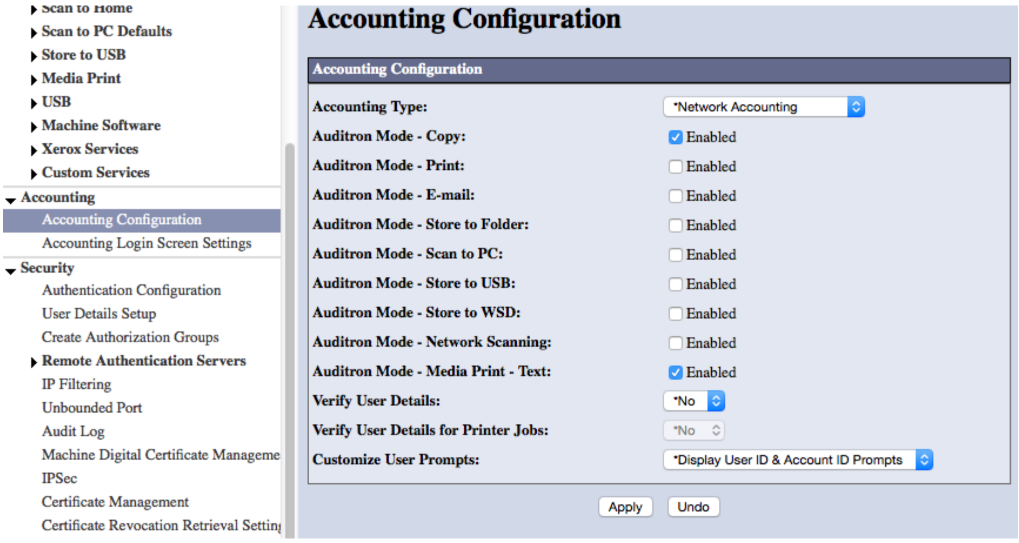
This is only applicable to multi-function devices.

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:

5.1.5.1 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.



Accounting Configuration

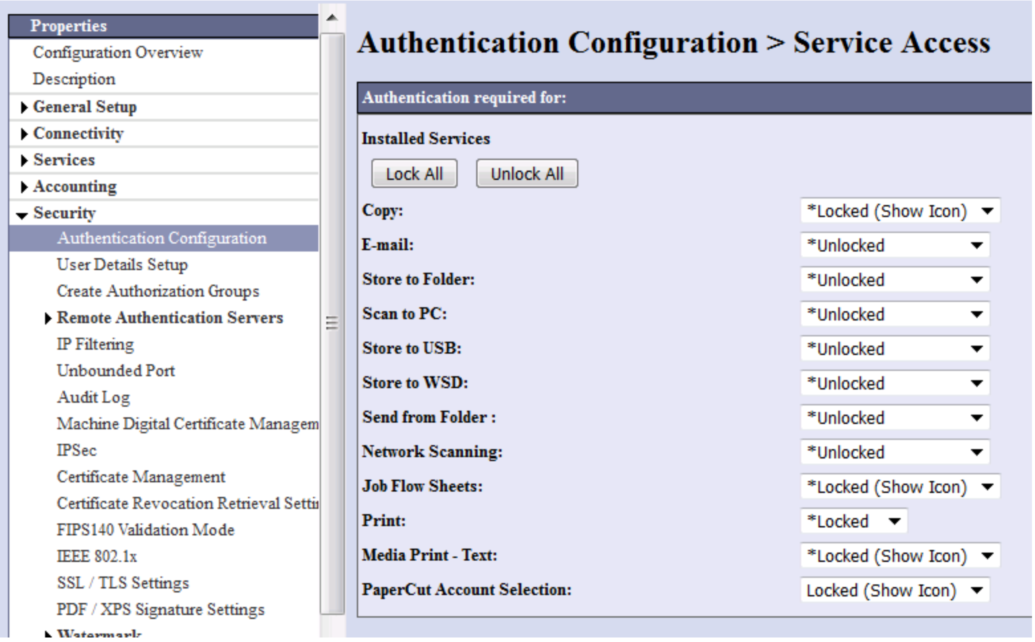
Accounting Configuration

Accounting Type: *Network Accounting
Auditron Mode - Copy: ☑ Enabled
Auditron Mode - Print: ☐ Enabled
Auditron Mode - E-mail: ☐ Enabled
Auditron Mode - Store to Folder: ☐ Enabled
Auditron Mode - Scan to PC: ☐ Enabled
Auditron Mode - Store to USB: ☐ Enabled
Auditron Mode - Store to WSD: ☐ Enabled
Auditron Mode - Network Scanning: ☐ Enabled
Auditron Mode - Media Print - Text: ☑ Enabled
Verify User Details: *No
Verify User Details for Printer Jobs: *No
Customize User Prompts: *Display User ID & Account ID Prompts

5.1.5.2 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

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



Authentication Configuration > Service Access

Authentication required for:

Installed Services

Copy: *Locked (Show Icon)
E-mail: *Unlocked
Store to Folder: *Unlocked
Scan to PC: *Unlocked
Store to USB: *Unlocked
Store to WSD: *Unlocked
Send from Folder : *Unlocked
Network Scanning: *Unlocked
Job Flow Sheets: *Locked (Show Icon)
Print: *Locked
Media Print - Text: *Locked (Show Icon)
PaperCut Account Selection: Locked (Show Icon)

5.1.6 Maximum of 30 concurrent fax jobs

This is only applicable to multi-function devices.

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

5.2 Faxing limitations summary

This is only applicable to multi-function devices.

5.2.1 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:

1. ColorQube 8700
2. ColorQube 8900
3. WorkCentre 5735/5740/5745/5755
4. WorkCentre 5765/5775/5790
5. WorkCentre 7525/7530/7535/7545/7556

5.2.2 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).

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.6.1 Turning Off Job Limits' Preauthorization

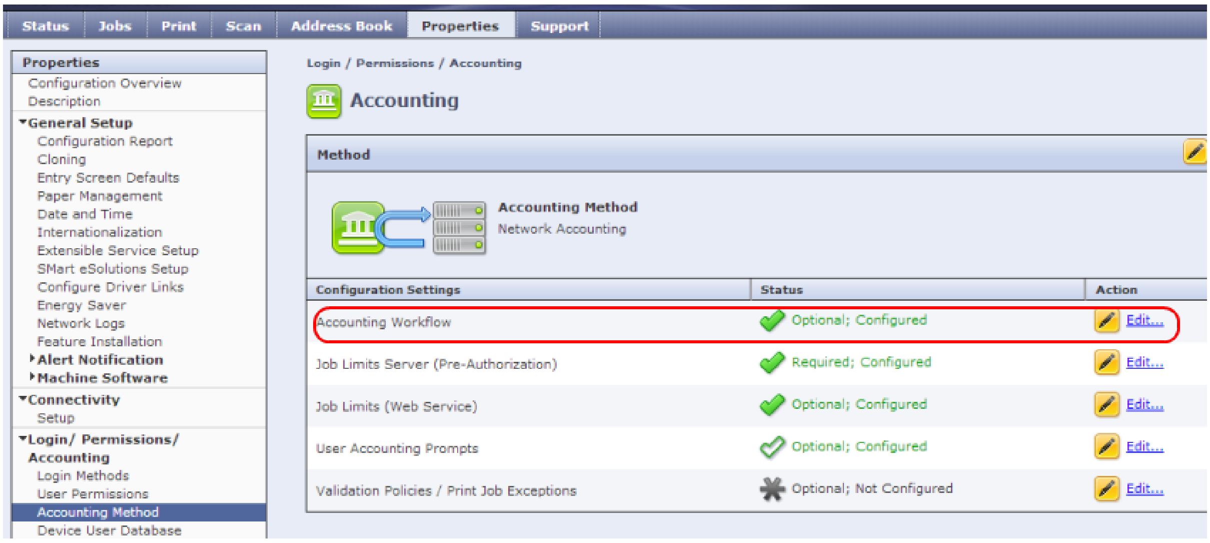
You need to do the following to disable the job limits from pre-authorizing jobs.

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.

5.6.1.1 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.

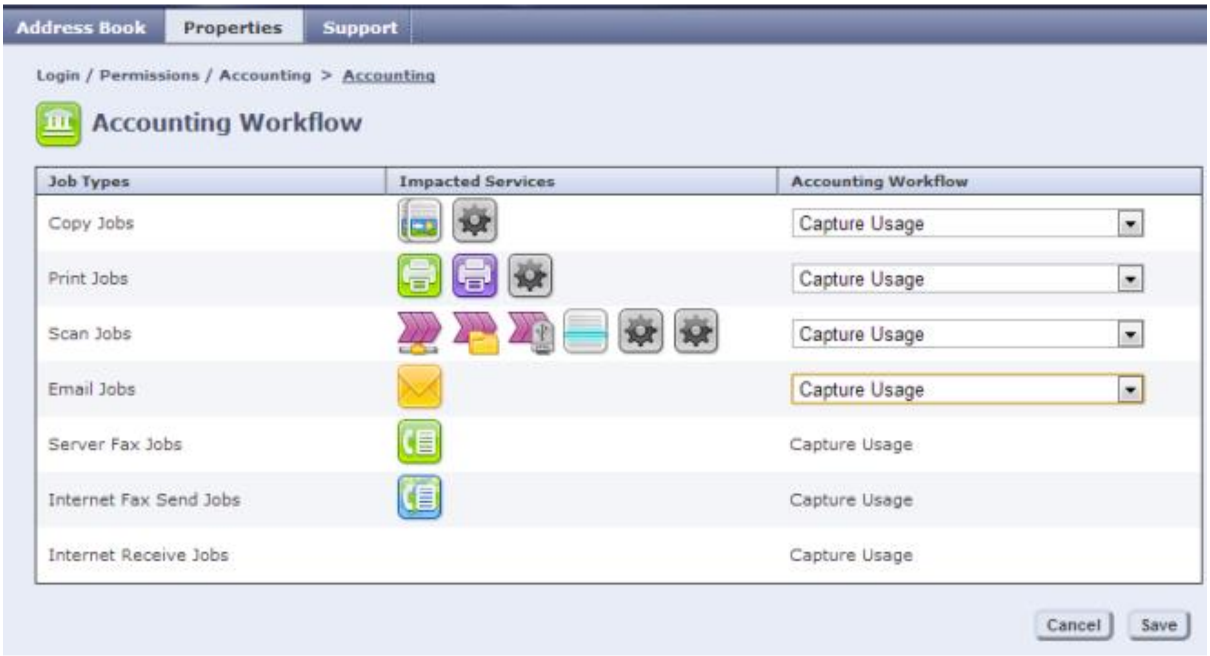
1. Login to the device's web admin (CWIS).
2. Navigate to Properties > Login/Permissions/Accounting > Accounting Method.
3. Click on the Edit button for Accounting Workflow.



Accounting Method
Network Accounting

Configuration Settings	Status	Action
Accounting Workflow	Optional; Configured	Edit...
Job Limits Server (Pre-Authorization)	Required; Configured	Edit...
Job Limits (Web Service)	Optional; Configured	Edit...
User Accounting Prompts	Optional; Configured	Edit...
Validation Policies / Print Job Exceptions	Optional; Not Configured	Edit...

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

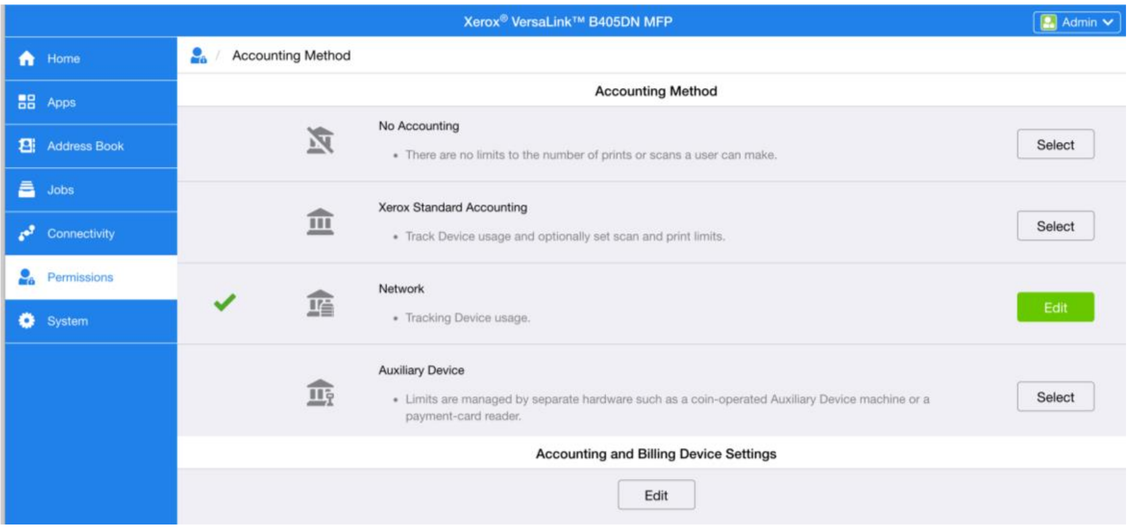


Job Types	Impacted Services	Accounting Workflow
Copy Jobs		Capture Usage
Print Jobs		Capture Usage
Scan Jobs		Capture Usage
Email Jobs		Capture Usage
Server Fax Jobs		Capture Usage
Internet Fax Send Jobs		Capture Usage
Internet Receive Jobs		Capture Usage

5.6.1.2 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**.



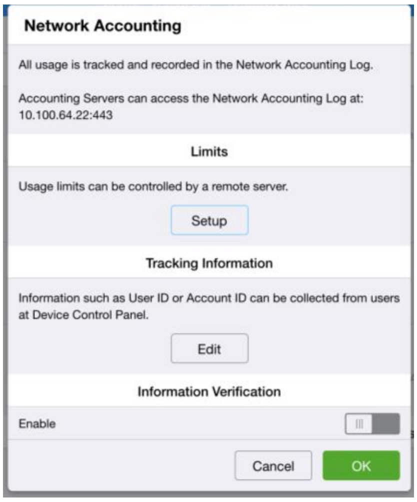
No Accounting
- There are no limits to the number of prints or scans a user can make.

Xerox Standard Accounting
- Track Device usage and optionally set scan and print limits.

✓ Network
- Tracking Device usage.

Auxiliary Device
- Limits are managed by separate hardware such as a coin-operated Auxiliary Device machine or a payment-card reader.

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



All usage is tracked and recorded in the Network Accounting Log.

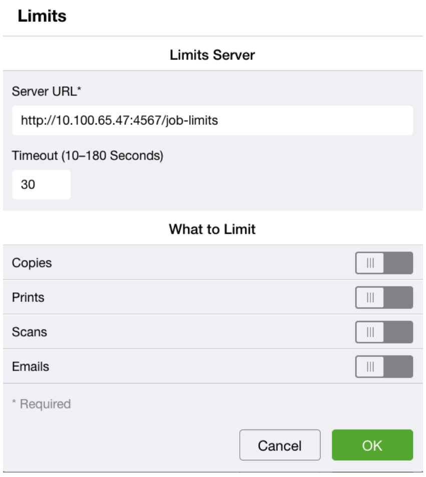
Accounting Servers can access the Network Accounting Log at: 10.100.64.22:443

Usage limits can be controlled by a remote server.

Information such as User ID or Account ID can be collected from users at Device Control Panel.

Enable: Off

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



Server URL*: http://10.100.65.47:4567/job-limits

Timeout (10–180 Seconds): 30

Copies: Off

Prints: Off

Scans: Off

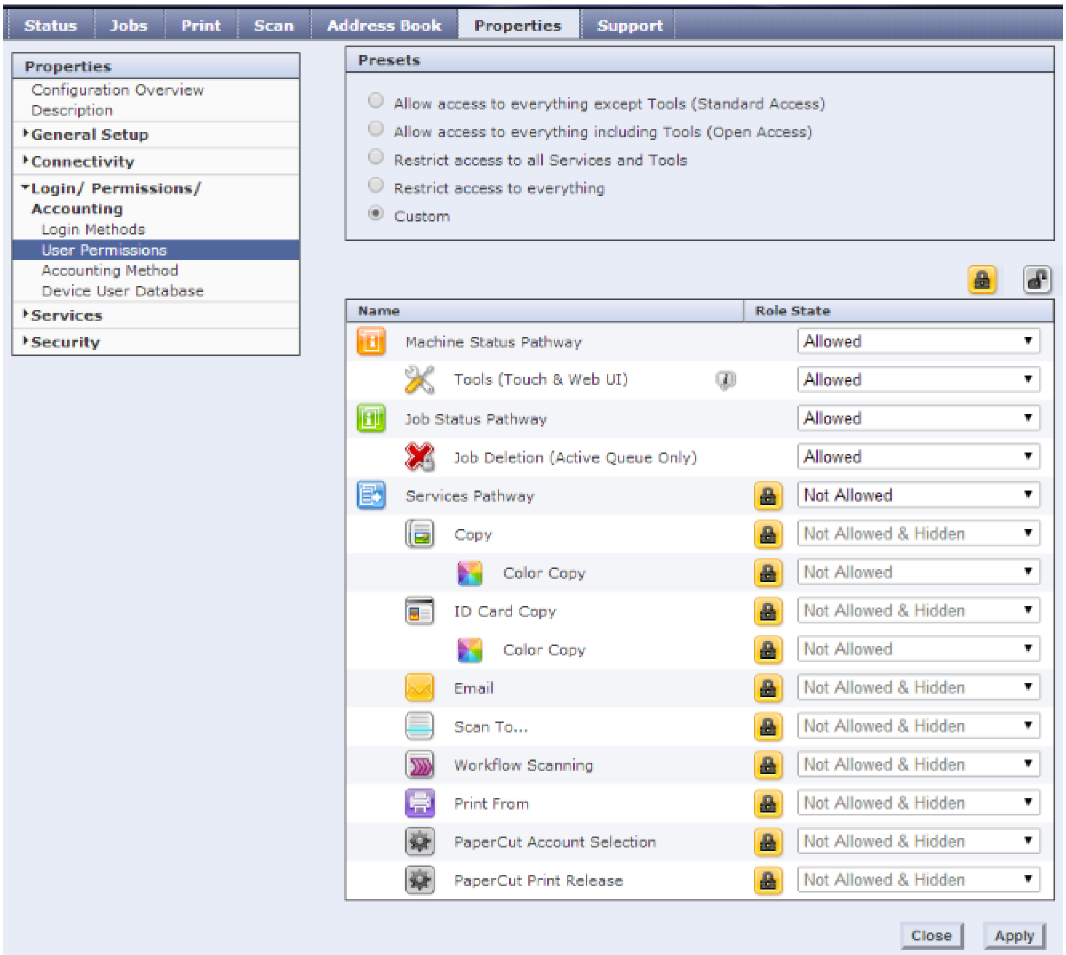
Emails: Off

* Required

6. Click `OK`.

5.7 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.

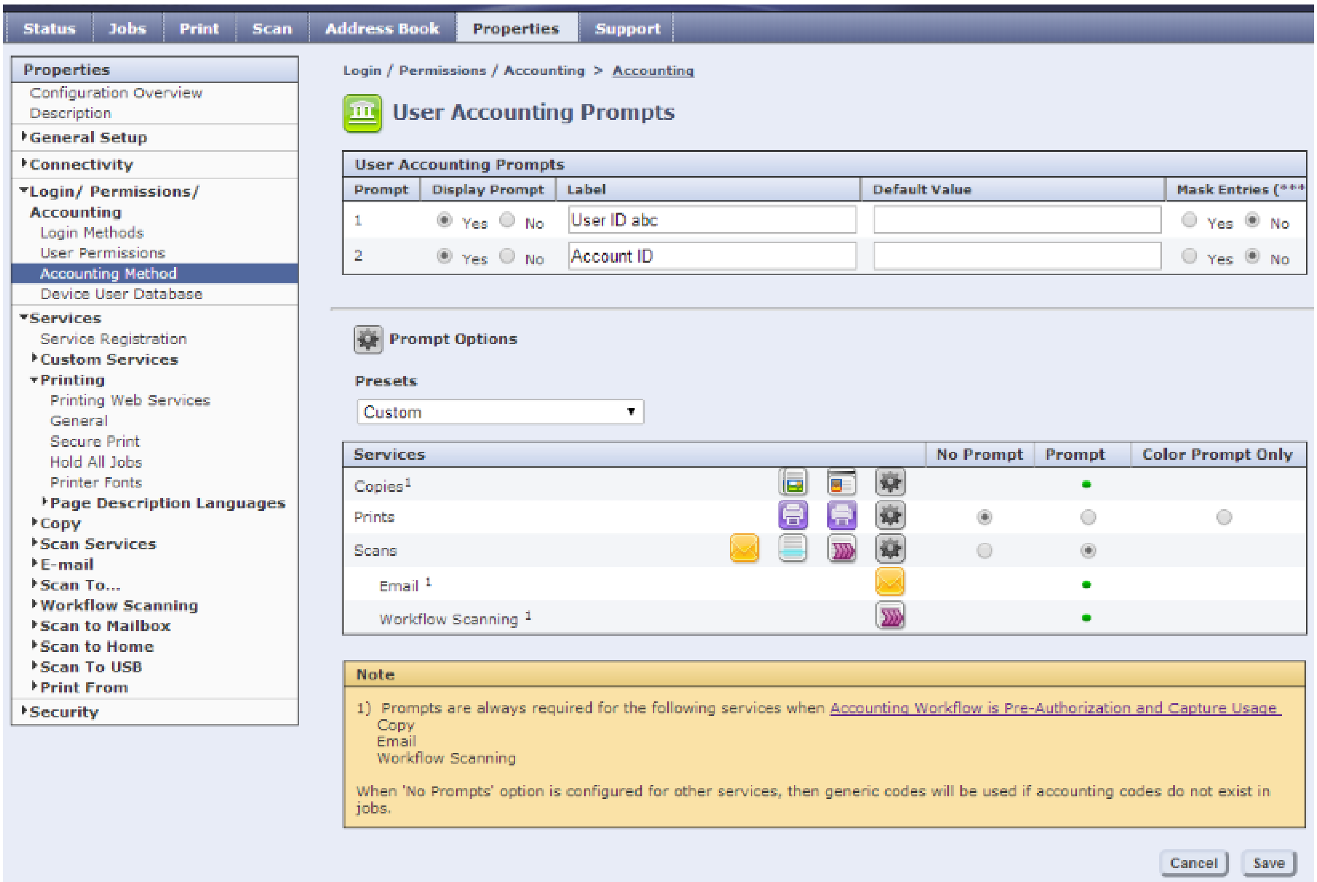


Presets

○ Allow access to everything except Tools (Standard Access)
○ Allow access to everything including Tools (Open Access)
○ Restrict access to all Services and Tools
○ Restrict access to everything
● Custom

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

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.



Login / Permissions / Accounting > Accounting

User Accounting Prompts

User Accounting Prompts

Prompt	Display Prompt	Label	Default Value	Mask Entries (***
1	● Yes ○ No	User ID abc		○ Yes ● No
2	● Yes ○ No	Account ID		○ Yes ● No

Prompt Options

Presets: Custom

Services	No Prompt	Prompt	Color Prompt Only
Copies[1]		●	
Prints	●	○	○
Scans	○	●	
Email [1]		●	
Workflow Scanning [1]		●	

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.

5.8 Integrated Scanning limitations summary

This is only applicable to multi-function devices.

- 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.

5.9 Phonebook contacts

The list of phonebook contacts visible on the MFD can be limited using the config key **system.scan.fax.contact.max-limit**. The default limit is set to 50.

6 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).

7 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 on the device’s web interface aligns with the configuration on the PaperCut MF Admin web interface.
- 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.

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, you must 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?

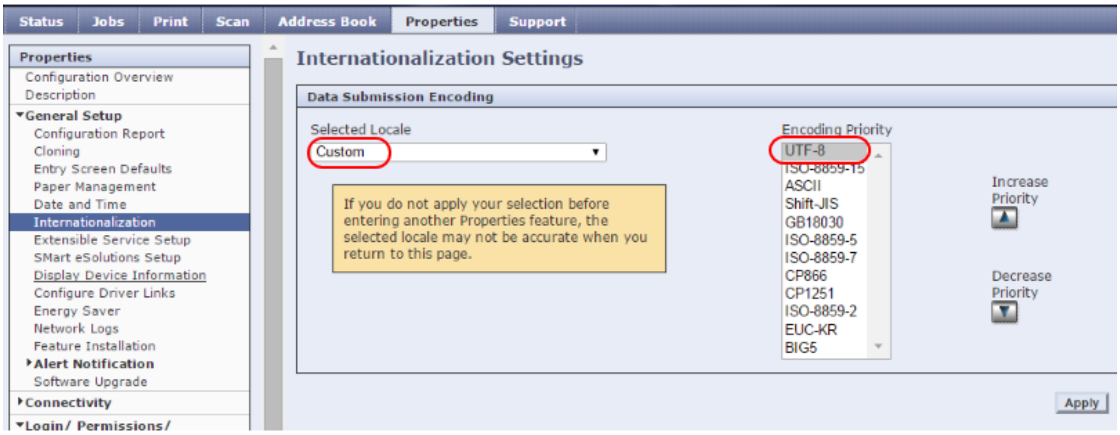
This should only be an issue on EIP 2.0+ devices and not on EIP 1.5 devices. The Job Assembly feature of the Xerox, unfortunately, is not compatible with Job Limits and therefore the Job Assembly buttons are disabled by default. If you need this functionality and don't need Zero Stop, then see section 5.6.

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



Internationalization Settings

Data Submission Encoding

Selected Locale: Custom

Encoding Priority:
UTF-8
ISO-8859-15
ASCII
Shift-JIS
GB18030
ISO-8859-5
ISO-8859-7
CP866
CP1251
ISO-8859-2
EUC-KR
BIG5

If you do not apply your selection before entering another Properties feature, the selected locale may not be accurate when you return to this page.

Can the device panel buttons be used for Integrated Scanning?

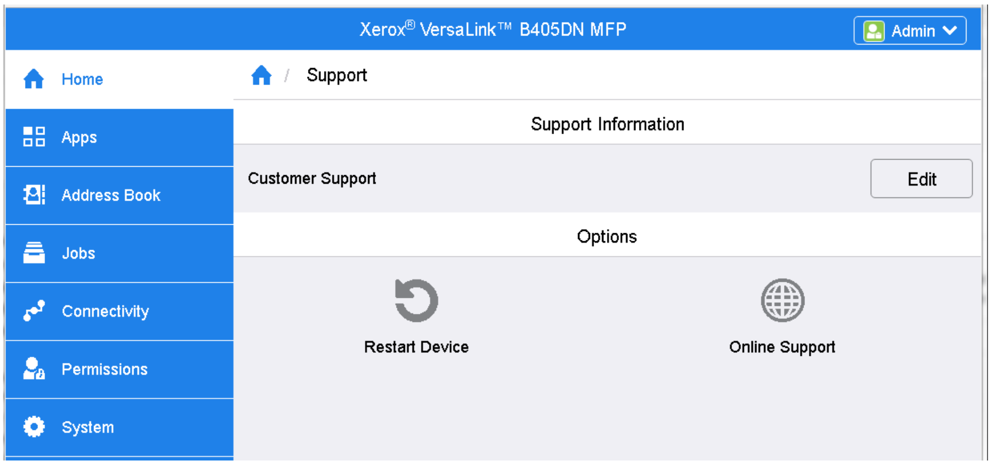
This is only applicable to multi-function devices.

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.

Device Status "Error: Xerox HTTP error calling"

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.

8 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.
    - To enable PaperCut MF to use:
        c. SNMPv1/v2c, ensure the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox is not selected (default).
        d. SNMPv3, select the **Use SNMPv3 for Toner Retrieval, Device Error Monitoring and Device Configuration** checkbox; and enter the following fields:
            - **Context name** – Do not enter any value.
            - **Username** – Enter **Xadmin**.
            - **Privacy password** – Enter the same value as the device web interface's **Privacy/ Encryption Password.**
            - **Authentication password** – Enter the same value as the device web interface's **Authentication Password.**
            - **Authentication protocol** – Select **MD5.**
            - **Privacy protocol** – Select **DES.**

9 Uninstallation

9.1 Temporarily disable *PaperCut MF - Xerox (Secure Access EIP 1.5+)*

To temporarily disable *PaperCut MF - Xerox (Secure Access EIP 1.5+)*:

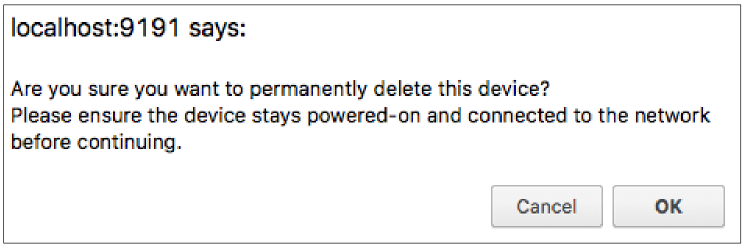
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In the **Configuration** area's **Enable/Disable**, select a **Disable** option.
5. Verify that *PaperCut MF - Xerox (Secure Access EIP 1.5+)* is disabled.
6. Verify that *PaperCut MF - Xerox (Secure Access EIP 1.5+)* is not available on the device to users.

9.2 Permanently uninstall *PaperCut MF - Xerox (Secure Access EIP 1.5+)*

To permanently uninstall *PaperCut MF - Xerox (Secure Access EIP 1.5+)*:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. Click **Actions > Delete this device**.

5. Click **Ok:**



localhost:9191 says:

Are you sure you want to permanently delete this device?
Please ensure the device stays powered-on and connected to the network before continuing.

6. Click **Devices** and verify that the device is no longer listed (*PaperCut MF - Xerox (Secure Access EIP 1.5+)* is permanently uninstalled).
7. Verify that *PaperCut MF - Xerox (Secure Access EIP 1.5+)* is not available on the device to users.
8. Only for VersaLink devices:
   a. Login to the web interface of the Versalink device as “Admin”
   b. Apps >> Print Release >> select “Delete App”
   c. Permissions >> Guest Access >> Device User Role >> select “Access All”
   d. Accounting Method >> No Accounting >> select “Change” then restart device