PaperCut MF - HP OXP Printer Only Embedded Manual

Contents

1 Document revision history

Published date or release	Details of changes made
22.0	5.5 In enhanced mode, pressing the 'Sign In' button before swiping an authentication card might cause unexpected behaviours
21.0	Enhanced workflow Introduction of new config keys
19.2.2	ext-device.hp-oxpd.login.id-field.numeric
19.2.0	Document restructure; other significant updates (2.4.5 Install PaperCut MF; 4.5 SNMP; 4.12.2 Header logo; 4.13 Config Editor)
18.3.6	3.4.1 Install PaperCut MF; 5.2 Security settings; 5.5.2 Device functions not controlled and tracked by PaperCut MF; 5.6 Manage Trays; 5.9 Device's first screen's message; 5.12 Config Editor; 8.4 Device's first screen and login workflow; 8.7 The HTTPS (SSL/TLS) setup does not work; 8.9 The ability to modify trays is unavailable; 8.9 The ability to modify trays is unavailable
18.3.4	5.4 "Swipe card" authentication method; 5.13 Config Editor
18.3.3	3.2 System, access, and device requirements
18.2.6	5.2 Security settings
18.2.4	5.4 "Swipe card" authentication method; 5.11 Config Editor
18.2.3	5.5 Device functions; 5.11 Config Editors; 8 FAQ & Troubleshooting
18.2.0	2 Overview; 3 Installation; 4 Post-install testing; 5 Configuration; 8 FAQ & Troubleshooting; 9 Appendix A: Device screens

18.1.1	3.1 Supported devices; 3.2 System, access, and device requirements; 5.2.1 HTTPS Security

2 Installation

This section covers the installation of *PaperCut MF - HP OXP Printer Only*.

2.1 Supported devices

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

2.2 Compatible devices

Ensure that supported HP devices on the network are compatible with PaperCut's embedded software solution *PaperCut MF - HP OXP Printer Only:*

- they are running HP FutureSmart 4.
  For more information, see 2.4.1 Log in to the device's web interface as an administrator and 2.4.2 Determine the device's HP platform

Note: This manual is only relevant to supported and compatible HP 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.

2.3 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 – 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 17.4.2.
- 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:
    - 7627 (TCP/HTTPS)
    - 80 (TCP/HTTP)
    - 443 (SSL/TLS/HTTPS)
- The firmware is v4.6 or greater if using the enhanced user flow.

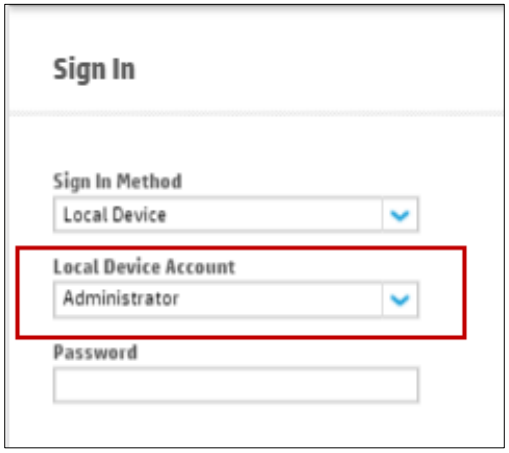
2.4 Setup procedure

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

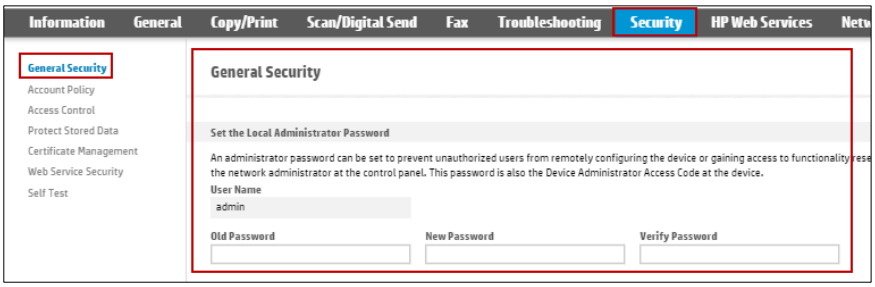
2.4.1 Log in to the device's web interface as an administrator

To access the device's web interface as an administrator:

1. Log in to the device's web interface.
2. In **Local Device Account**, select **Administrator**:

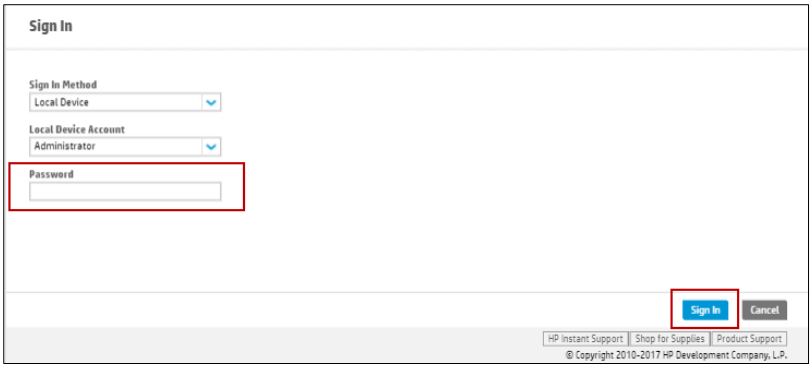


3. If this device's web interface is being accessed for the first time:
    a. Do not enter a password
    b. Click **Sign in**.
    c. Navigate to **Security > General Security**.
    d. Set the administrator credentials:



    e. Click **Apply**.
4. If this device's web interface has been accessed previously:
    a. Enter the administrator password.

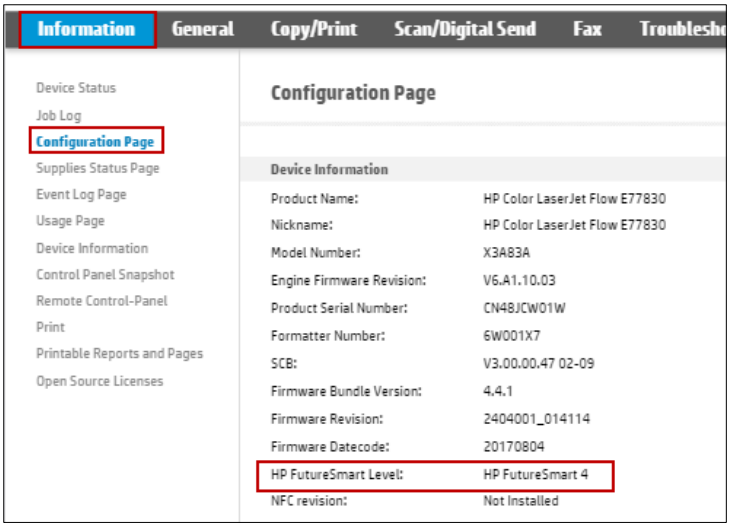
b. Click **Sign in**:



2.4.2 Determine the device's HP platform

To determine the device's HP platform:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Information > Configuration Page.**
3. Verify that the **Device Information** area's field **HP FutureSmart Level** displays **HP FutureSmart 4**:



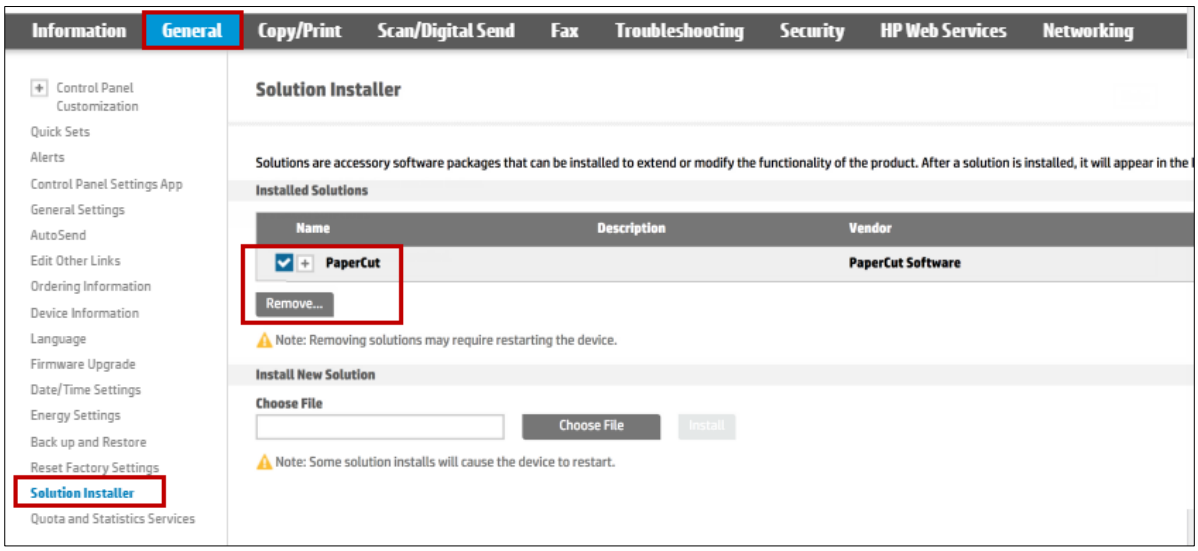
Note: This manual is only relevant to supported HP FutureSmart 4 devices. For more information on PaperCut's embedded software solutions for other devices and platforms, contact your reseller or Authorized Solution Center. You can find their contact information in your PaperCut MF Admin web interface, on the **About** page.

2.4.3 Uninstall PaperCut MF - HP FutureSmart Legacy

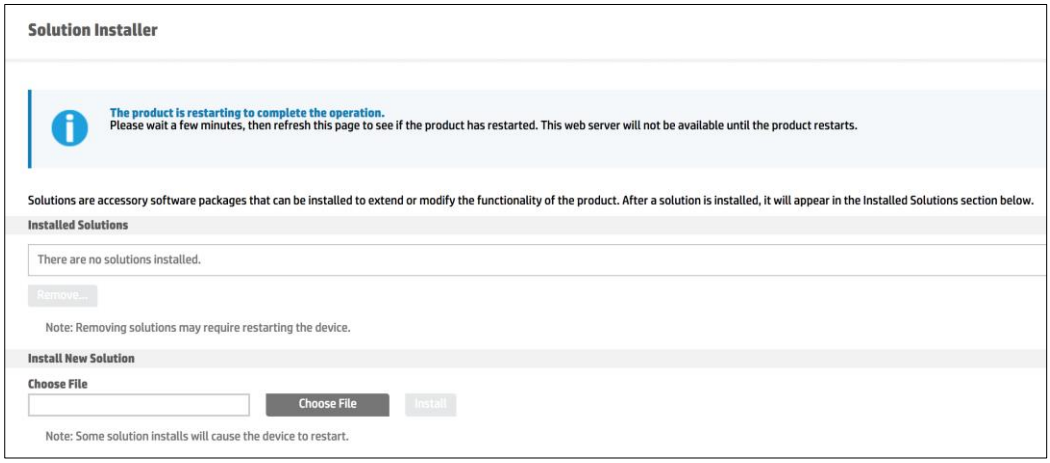
If PaperCut's embedded software solution *PaperCut MF - HP FutureSmart Legacy* is already installed, then ensure to first uninstall it before attempting to install *PaperCut MF - HP OXP Printer Only*.

To uninstall *PaperCut MF - HP FutureSmart Legacy*:

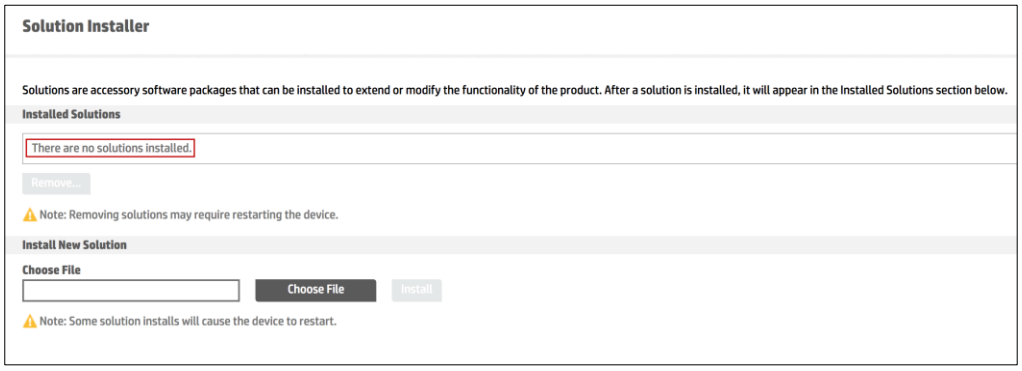
1. Log in to the device's web interface as an administrator.
2. Navigate to **General > Solution Installer.**
3. Select **PaperCut**.
4. Click **Remove…**



The device reboots and restarts to uninstall *PaperCut MF - HP FutureSmart Legacy* from the device:



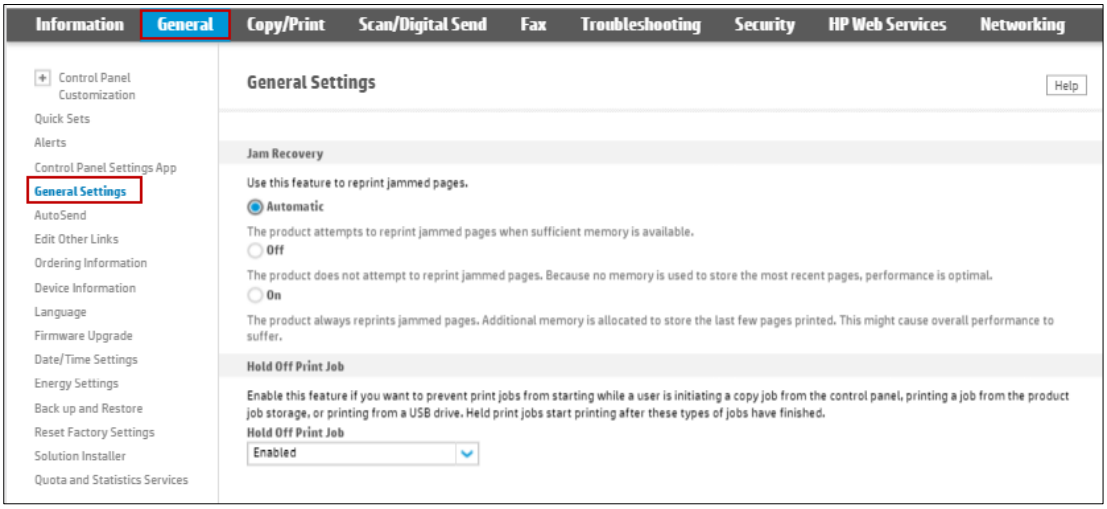
5. Verify that *PaperCut MF - HP FutureSmart Legacy* is uninstalled from the device:



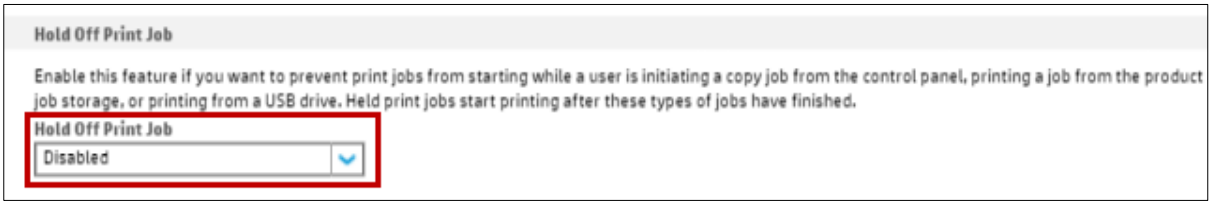
2.4.4 Configure the device's Hold Off Print Job settings

To configure the device's Hold Off Print Job setting:

1. Log in to the device's web interface as an administrator.
2. Navigate to **General > General Settings**:



3. Change the **Hold Off Print Job** setting from **Enabled** to **Disabled**.
   Note: This setting is enabled by default, delaying printing by 15 seconds.



4. Click **Apply**.

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

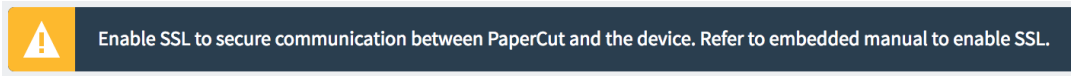
Note: If you are running a version prior to PaperCut MF 19.2.0, then this is the only applicable option.

To install PaperCut MF on each device:

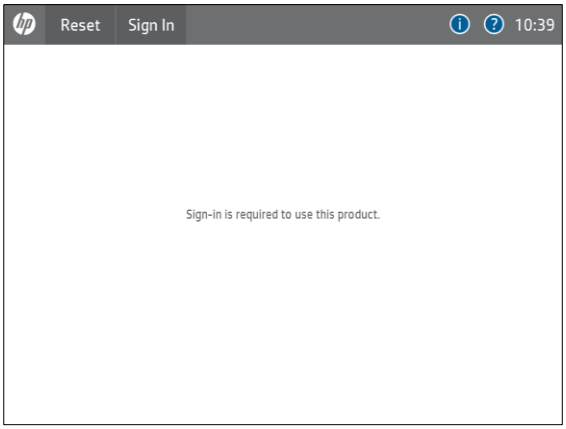
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices.**
3. Click **Create Device.**
4. In **Type**, select **HP OXP (Printer Only).**
5. In **Device name**, enter a descriptive name for the device.
6. Optionally, in **Location/Department**, enter location or department details of 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. For more information, see 2.4.1 Log in to the device's web interface as an administrator.
9. In **Function**, select the required device jobs:
   - **Track & control copying**
   - **Enable print release**

   Note: For more information, see 4.6 Secure print release and 4.7 Device jobs.
10. Click **Ok**.
11. 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**:

      Note:
      - If the **Device Status** displays any other status, see 6.2 Device Status "Started (with errors)", 6.3 Device Status "Stopped (with errors)"
      - If the PaperCut MF Admin web interface displays the following warning, then see 4.2.1 HTTPS Security (recommended):

    - If the device's **HP FutureSmart 4 Firmware Bundle Version** is **4.5.5 or above**, then the device displays a white screen with the following default message (to customize this message, see 4.11 Device's first screen's message):

Clicking **Sign In**, displays the PaperCut MF Login screen.

- **Note:** If the device's **HP FutureSmart 4 Firmware Bundle Version** is **below 4.5.5**, then see 6.4 Device's first screen and login workflow.

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:

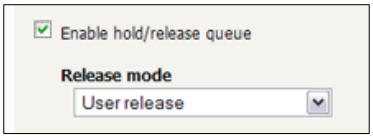
1. To ensure that PaperCut MF works as expected.
2. To familiarize yourself with the features and functionality of PaperCut MF.

This section covers the following post-install testing scenario for *PaperCut MF - HP OXP Printer Only*:

- 3.2 Simple printing

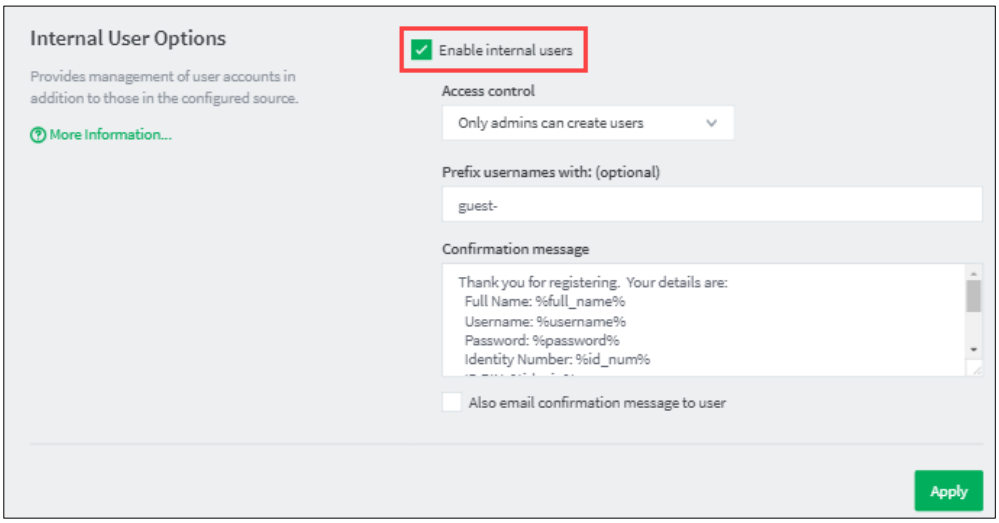
3.1 Test preparation

To execute the post-install testing scenario, ensure the following requirements are met:

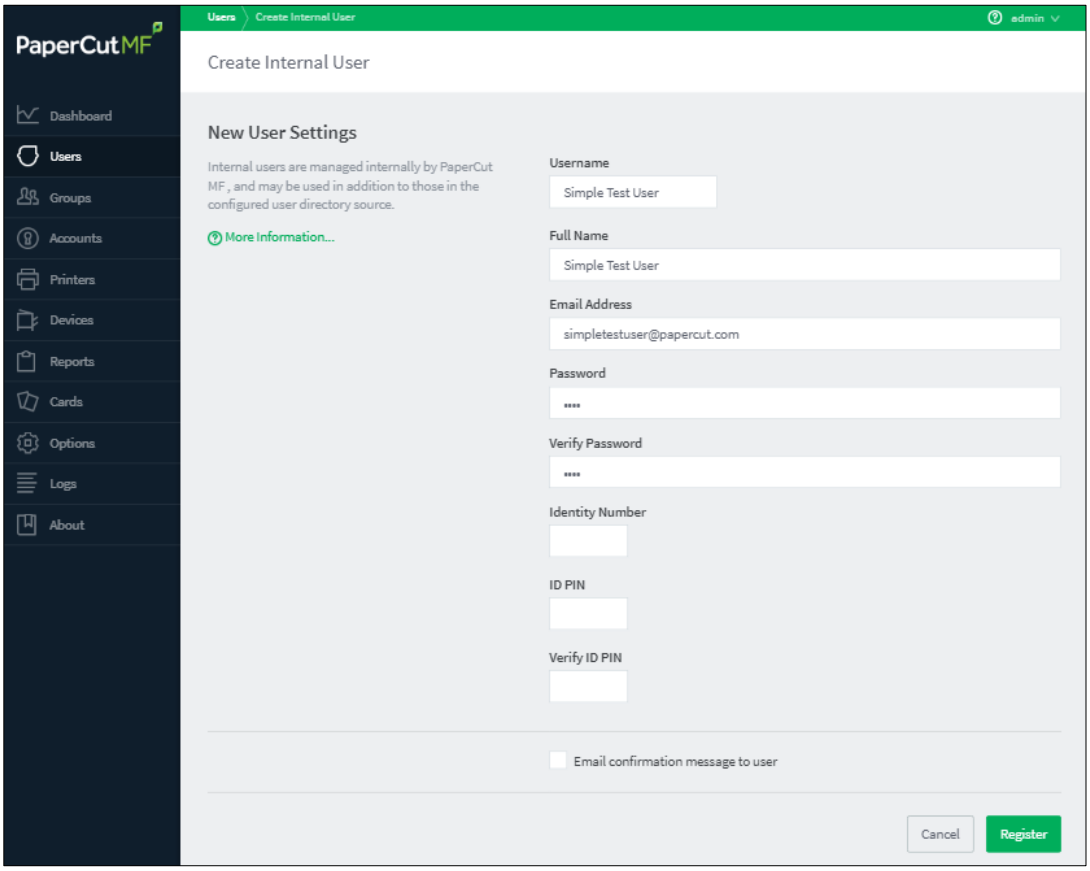
- **Printer queue settings** - The printer queue's Hold/Release Queue Settings are configured. For more information, see the PaperCut MF manual.
  To configure the printer queue's Hold/Release Queue Settings:
  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Printers**.
  3. Select the Printer that is applicable to the device being tested.
  4. In the **Hold/Release Queue Settings** area, select the **Enable hold/release queue**.
     

  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.
- **Simple test user** - A simple test user who performs simple printing is created and configured.
  To create and configure a test user:
  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**.

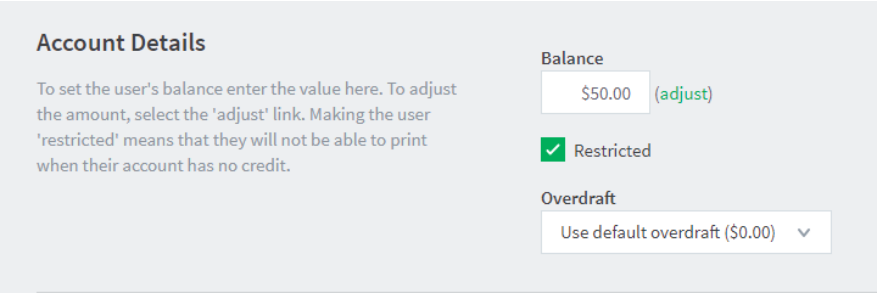


5. Navigate to **Users**.
6. Click **Create internal user…**
7. Enter the relevant details for the test users as required (simple test user):

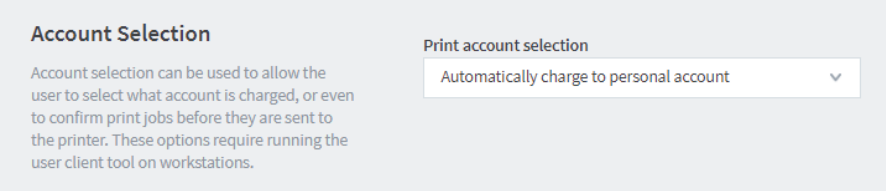


8. Click **Register**.
9. Navigate to **Users**.
10. From the **User List**, select the simple test user.

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



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



13. Click **Apply**.

3.2 Simple printing

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

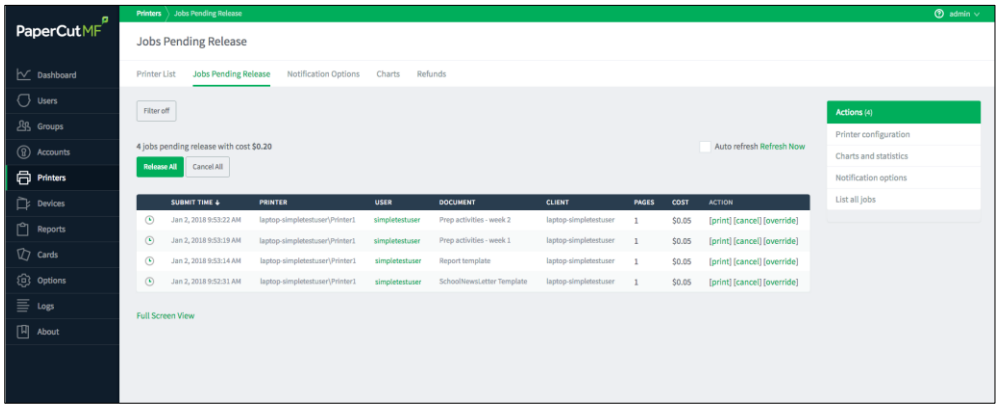
To test simple printing, ensure the following requirements are met:

- **Printer queue settings**
- **Device functions**
- **Simple test user**

For more information, see 3.1 Test preparation.

To test simple printing:

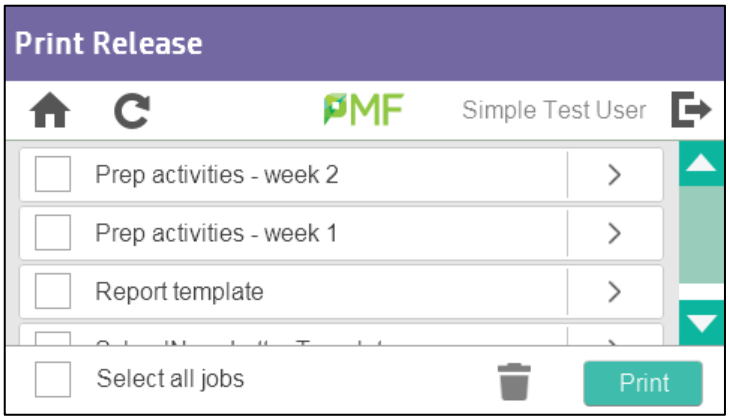
1. Log in to a computer as the simple test user.
2. Print a few jobs to the source queue that was selected in the **Devices > External Device List > Device Details > Print Release > This device will display jobs for release from the selected source queues** area of the device being tested.
3. Log in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



6. Log out of the PaperCut MF Admin web interface.
7. Log in to the device as the simple test user:

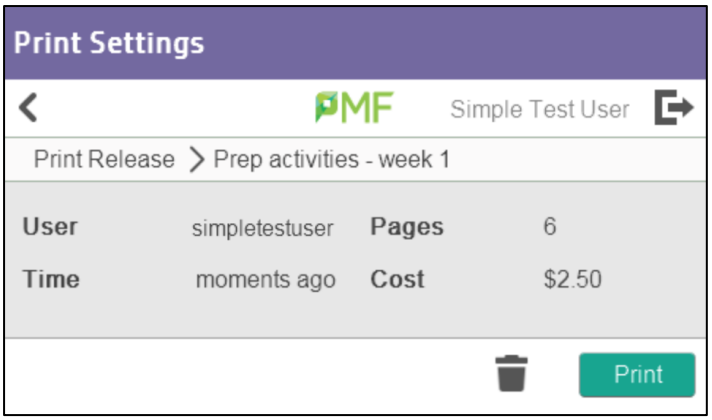
8. Select **Print Release**:

9. Verify that the print jobs for the simple test user are being held and listed:

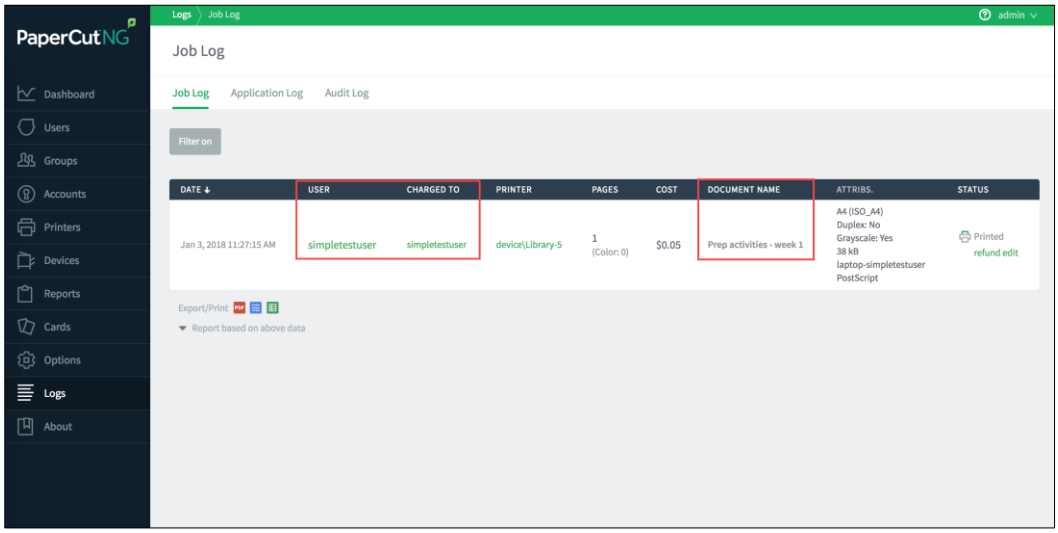


10. To release one or many held print jobs at once, select all the relevant held print jobs and click **Print**.
11. To delete one or many held print jobs at once, select all the relevant held print jobs and click the **Bin** icon.
12. To view and take actions on a single held print job, click the chevron:

Details of the held print job are displayed:



13. Log out of the device.
14. Log in to the PaperCut MF Admin web interface.
15. Navigate to **Logs**.
16. 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:



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

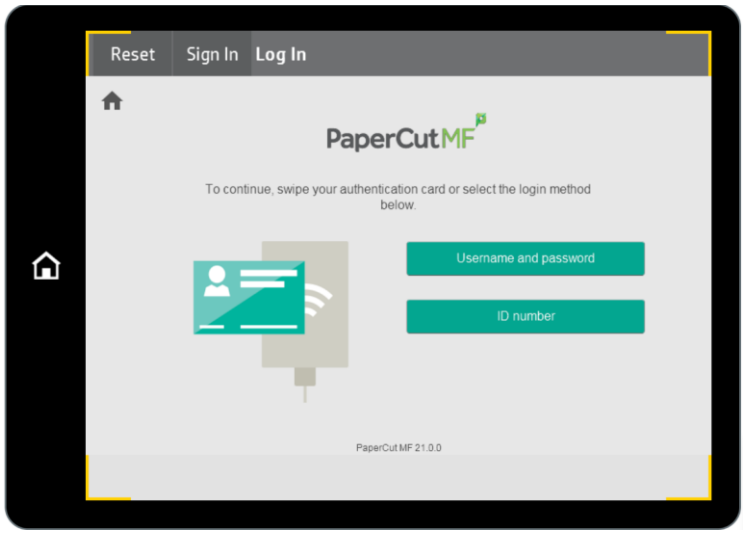
3.3 Enhanced user workflow

HP Enhanced mode can be enabled via a config key ext-device.hp-oxpd.enhanced-mode. This user workflow presents PaperCut login and directs user to PaperCut home screen. When disabled, user workflow presents PaperCut login and directs user to Device home screen.

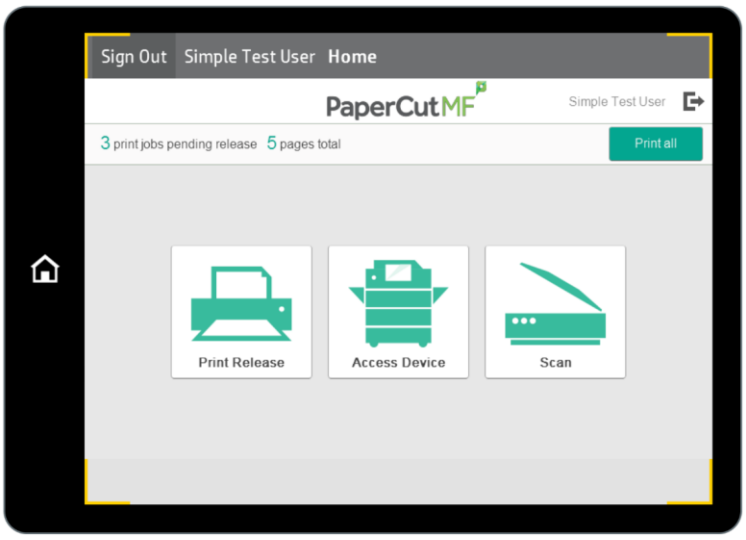
3.3.1 Printing

When testing the simple print workflow, the enhanced user flow at the device is altered as follows:

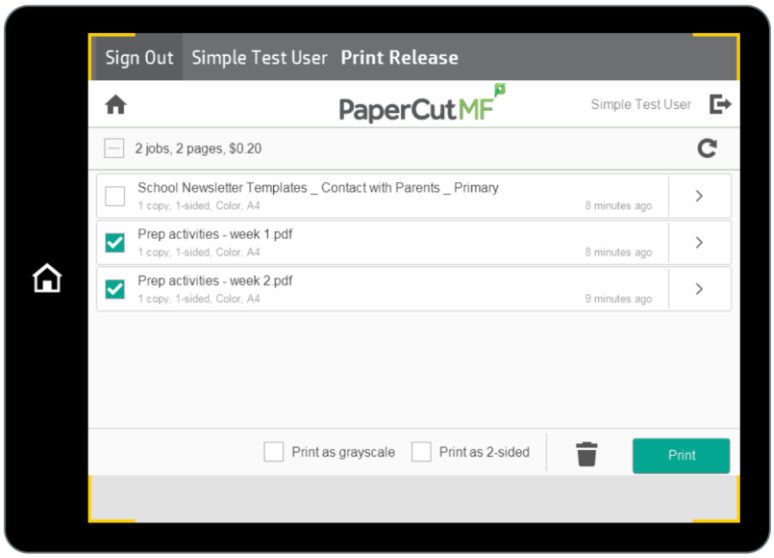
1. Log in to the device as the simple test user:



2. Select **Print Release**:

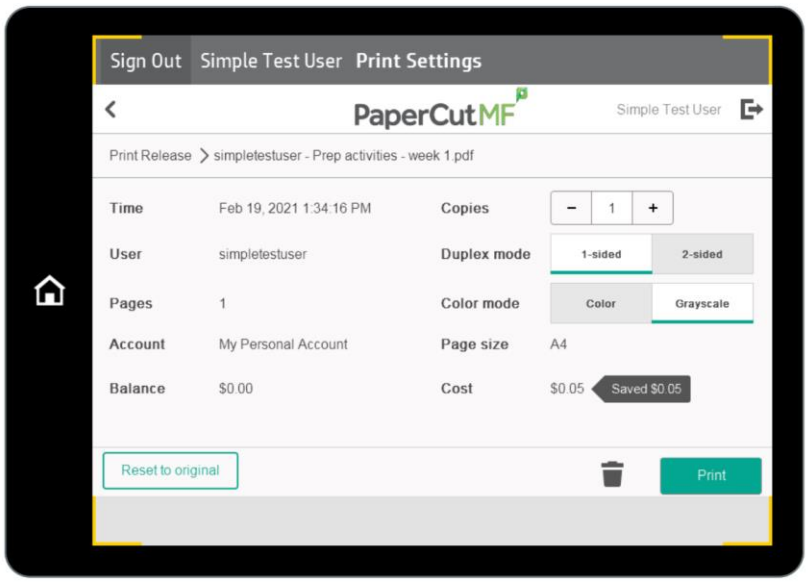


3. Verify that the print jobs for the simple test user are being held and listed:



4. To release one or many held print jobs at once, select all the required held print jobs and click **Print**.
5. To delete one or many held print jobs at once, select all the required held print jobs and click the **Bin** icon.
6. To view and take actions on a single held print job, click the chevron:

Details of the held print job are displayed:



7. Log out of the device.

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 - HP OXP Printer Only*.

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 4.13 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:

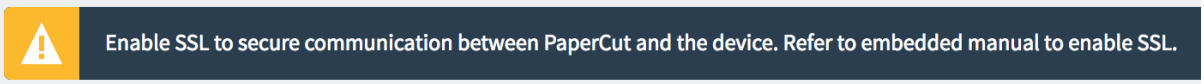
1. Site Servers must already be installed and configured. For more information, see the PaperCut MF manual.
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Sites**.
4. Select the Site Server.
5. In the **Configuration** area, enter the IP address or DNS name of the PaperCut MF Site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

4.2 Security settings

4.2.1 HTTPS Security (recommended)

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

Note: Until HTTPS is configured, the following warning is displayed on the PaperCut MF Admin web interface:



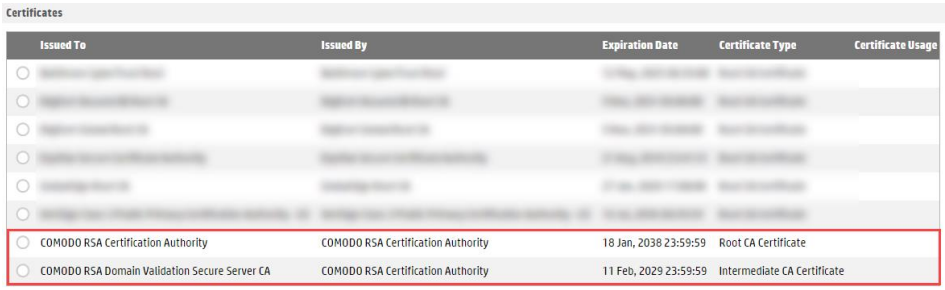
To enable HTTPS, you must have an SSL certificate installed on the PaperCut MF Application Server. The certificate must use the server's fully-qualified domain or IP address. This must be defined either in the **Common Name** (CN) field or included in the **Alternative Names** (AN) of the subject of the certificate. Without this, the device cannot connect to the server, since devices do not work with hostname-only certificates (i.e. not fully qualified).

You can use either a **self-signed SSL certificate** or a **CA-signed SSL certificate**:

- **Self-signed SSL certificate –** To use a self-signed SSL certificate that is generated by default when installing PaperCut MF:
    1. Regenerate it using PaperCut MF's `create-ssl-keystore` tool in: `[PaperCut MF Install Location]\server\bin\[platform]`
       Note: When regenerating it, ensure:
       - to include the command's required parameters and arguments.
           - On newer HP Gemstone devices, you may need to set the country code by using the Country (C) key of the `RDN` parameter to ensure that the certificate is valid.
       - that the `<SYSTEM-NAME>` parameter contains the same Fully Qualified Domain Name (or IP address) as that of the config key **system.network-address**. For example, `"myserver.fullname.com".` This is because the default self-signed certificate generated during PaperCut MF installation (device registration and integration) is issued using a hostname, instead of the IP address.
       - that the keystore location always contains only one, most recently generated self-signed certificate.

       For more information, see the PaperCut MF manual.
    2. Restart the PaperCut MF Application Server.
    3. Set the config key **ext-device.hp-oxpd.use-ssl** to **Y**. For more information, see 4.13 Config Editor.
    4. It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 4.13 Config Editor.
- **CA-signed SSL certificates –** To use a CA-signed SSL certificate (for example, Verisign, Thawte):
    1. Ensure that the `<SYSTEM-NAME>` parameter contains the same Fully Qualified Domain Name (or wildcard) as that of the config key **system.network-address**. This is because Certificate Authorities generally no longer accept certificate requests for either intranet names or IP addresses. For more information, see the PaperCut MF manual.
    2. Set the config key **ext-device.hp-oxpd.use-ssl** to **Y**. For more information, see 4.13 Config Editor.
    3. It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 4.13 Config Editor.
    4. Log in to the device's web interface as an administrator.
    5. Navigate to **Security > Certificate Management**.
    6. In the **CA Certificates > Certificates** table, verify that the relevant Root and any required Intermediary Certificates are listed.

For example:



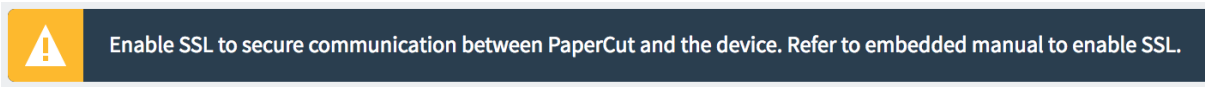
Note:

- If the relevant Root Certificate is not listed, click **Choose File**; select the relevant Root Certificate, click **Open**, and then click **Install**.
- If the relevant Intermediary Certificate is not listed, click **Choose File**; select the relevant Intermediary Certificate, click **Open**, and then click **Install**.

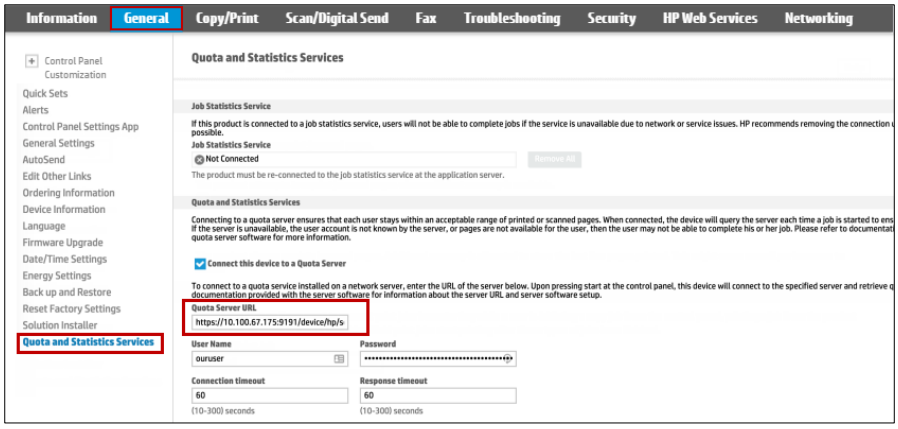
Note: After attempting to enable HTTPS, if the **Device Status** displays **Started (with errors) – Unknown error**, then see 6.7 Device Status "Started (with errors) – Certificate error".

To test HTTPS:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. Verify that the following warning message is not displayed:



5. Log in to the device's web interface as an administrator.
6. Navigate to **General > Quota and Statistics Services**.
7. Verify that **Quota Server URL** displays the URL as HTTPS and that its Fully Qualified Domain Name (or IP address) is the same as that of the config key **system.network-address**



8. Verify that you are able to log in to the device as a test user (simple test user).

4.2.2 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:

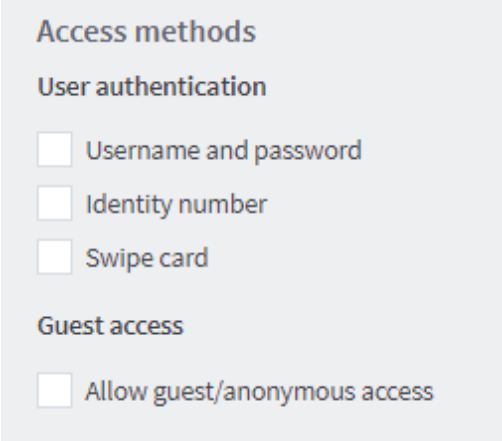
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **Security** area's field **Allowed device IP addresses**, enter a comma-separated list of device IP addresses or subnets (<ip-address1 or subnet-mask1>, <ip-address2 or subnet-mask2>).
4. Click **Apply**.

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:



   Note: You may use any one or a combination of all the available user authentication options, including the anonymous access authentication option. However, you cannot use the guest access authentication option. For more information, see 5.3 Guest access authentication is unavailable.

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 4.13 Config Editor. • **Configure HP Universal USB Proximity Card Reader (P/N:X3D03A):** If you use the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader, then you must select this. You must configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader to read the card types being used. For more information, see 4.13 Config

	Editor. With this option, users use their registered swipe card on the configured HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader
Allow guest/anonymous access	With this option: • All other options are automatically disabled and cannot be used as authentication options on the device. For more information, see 5.3 Guest access authentication is unavailable. • Users are authenticated as 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 anonymous users on the device. • Anonymous users 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:

1. Ensure the card reader is a supported card reader (see 4.4.1 Supported card readers).
2. The config key **ext-device.hp-oxpd.register.card-reader** is automatically set to **Y**, to allow PaperCut MF to register and establish an exclusive lock on card readers that are detected on the device. For more information, see 4.13 Config Editor.
3. The config key **ext-device.hp-oxpd.fast-swipe-login-flow** is automatically set to DEFAULT (N), to disable quick swipe-to-login. For more information, see 4.13 Config Editor.
4. The config key key **ext-device.hp-oxpd.skip-hid-restart** is automatically set to DEFAULT (N), to disable HID restart when a user logs in with a swipe card. For more information, see **Error! Reference source not found. Error! Reference source not found.**.

4.4.1 Supported card readers

PaperCut MF - HP OXP Printer Only supports the following configured and compatible card readers:

- Elatec TWN3 HID Prox
- Elatec TWN3 iCLASS
- Elatec TWN3 Mifare
- Elatec TWN4 Mifare
- HP Proximity Reader (CZ208A)
- HP Proximity Reader (CE931A)
- HP Proximity Reader (CE983A)
- HP Universal USB Proximity Card Reader (Part Number X3D03A)
- RF IDeas RDR-805H1AKU
- RF IDeas RDR-805H3AKU
- RF IDeas RDR-805T1AKU
- RF IDeas RDR 80581AKU-PPCT
- Securakey ET4-AUS-D

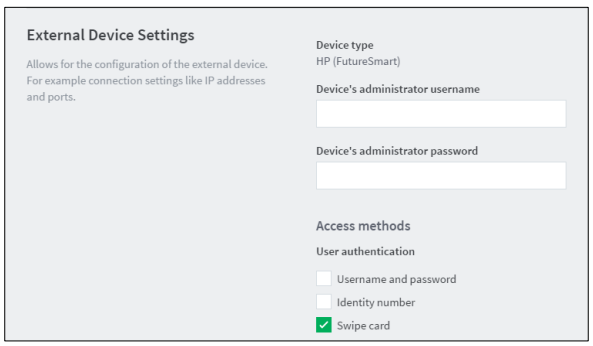
Note: In addition to the above card readers, you may configure *PaperCut MF - HP OXP Printer Only* to support other card readers by using the config key **ext-device.hp-oxpd.additional-card-readers.vid-pid.hex**. For more information, see 4.13 Config Editor.

4.4.2 HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader

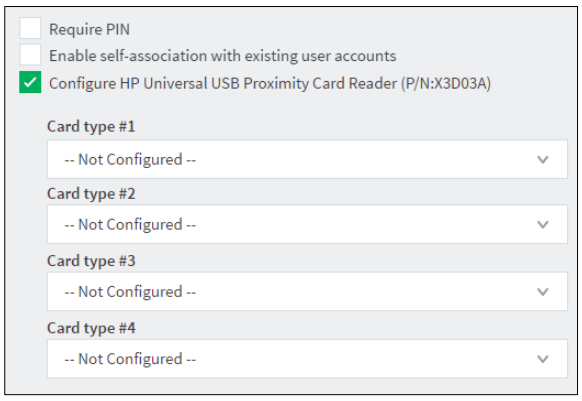
If the **Swipe card** authentication option is selected and you are using the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader, then you must configure it to read the card types being used. This is because your card reader's existing configurations are cleared and reset during PaperCut MF installation (device registration and integration).

To configure your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader:

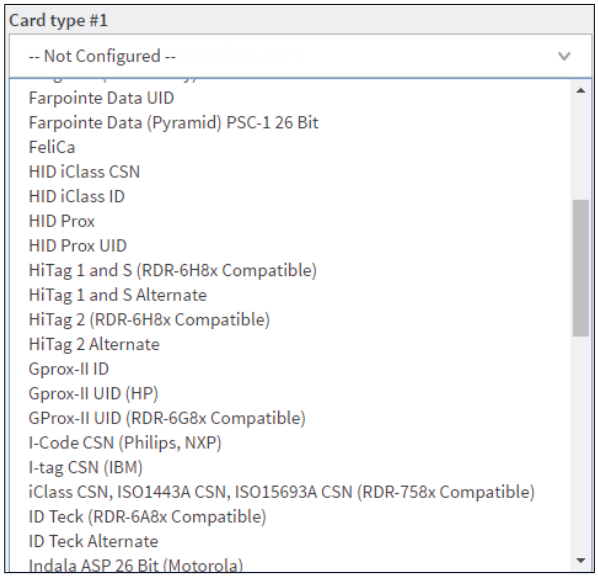
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In the **External Device Settings**, select the **Swipe card** user authentication access option:



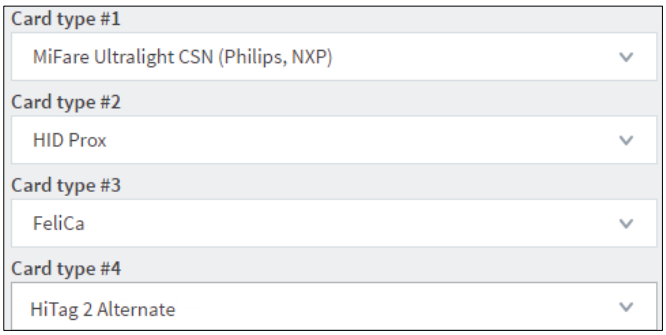
5. Select **Configure HP Universal USB Proximity Card Reader (P/N:X3D03A).**



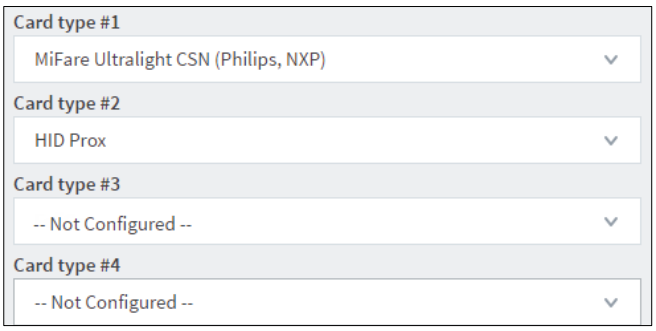
6. Select the card type to be read by your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU card reader:



- You can configure up to four card types:



- If you are not using all four card types, select "--Not Configured--" for the unused card types.



- Some card types conflict with other card types. Hence, avoid selecting such conflicting card types, because this causes some problems if using swipe card authentication for logging in and self-association. For more information, see 6.5 Swipe card authentication anomalies.

7. Click **Apply**.
8. Verify that your card reader can read the card types configured.

Note: Your card reader's configuration is reset and you must re-configure your card reader every time any one of the following occurs:

- your card reader is disconnected from and reconnected to your device's USB port
- your device is restarted
- your PaperCut MF Application Server is restarted
- your device's details are modified on the PaperCut MF Admin web interface's **Device Details** page

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 card identifiers using regular expression filters, use the config keys **ext-device.self-association-allowed-card-regex** and **ext-device.card-no-regex**. For more information, see 4.13 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 1234532929291221

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 4.13 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 4.13 Config Editor.

4.5 SNMP

PaperCut MF uses SNMP to:

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

By default, PaperCut MF uses SNMPv1/v2c to perform these actions. You can, however, select to use SMPv3 for better security and encryption.

For more information about SNMP, see the PaperCut MF manual.

To configure PaperCut MF to use SNMP:

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

4.6 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 account.

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.

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 and then proceed to release them.

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.

4.7 Device jobs

Device jobs include jobs initiated at the device, such as on-device print jobs.

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 **Track & control copying** to allow PaperCut MF to track and control on-device print jobs.

Note: Ensure this does not contradict the settings configured for the additional device jobs (see 4.7.1.1 Additional device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.

"Quota service error").

4.7.1.1 Additional device jobs

The device also offers some additional jobs, which you can configure access permissions for, using any one of the following options:

- 4.7.1.1.1 Using PaperCut MF
- 4.7.1.1.2 Using the device's web interface

4.7.1.1.1 Using PaperCut MF

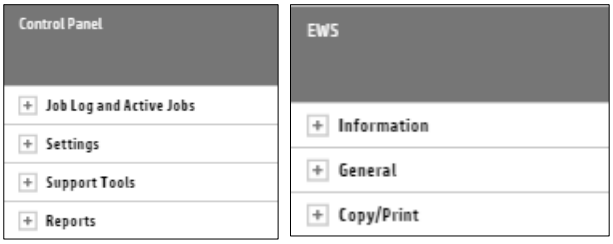
To configure access permissions for the additional device jobs using PaperCut MF:

1. Set the config key **ext-device.hp-oxpd.permission.server-managed** to **Y**. For more information, see 4.13 Config Editor.
2. To specify the additional device jobs that:
   - only authenticated users can access, use the config key **ext-device.hp-oxpd.permission.whitelist.** For more information, see 4.13 Config Editor.
   - unauthenticated users can access, use the config key **ext-device.hp-oxpd.guest.permission.whitelist**. For more information, see 4.13 Config Editor.

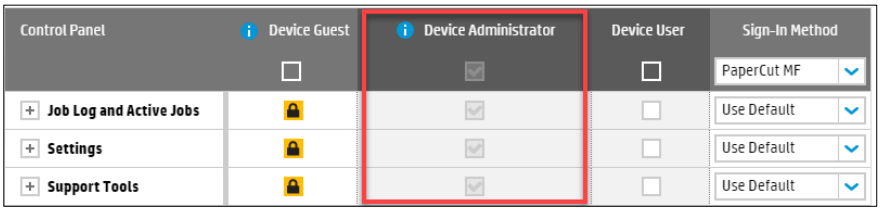
4.7.1.1.2 Using the device's web interface

To configure access permissions for the additional device jobs using the device's web interface:

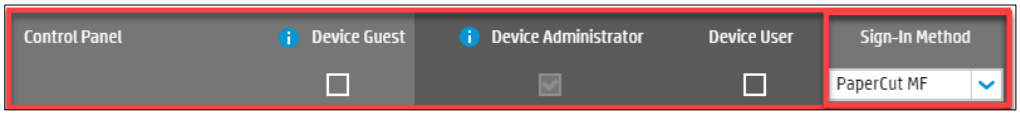
1. Ensure the config key **ext-device.hp-oxpd.permission.server-managed** is set to **N.** For more information, see 4.13 Config Editor.
2. Log in to the device's web interface as an administrator.
3. Navigate to **Security > Access Control > Sign-In and Permission Policies.**
   - The **Control Panel** and **EWS** columns display rows of all the additional device jobs:



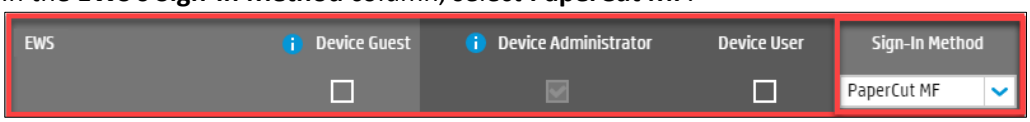
   - By default, all authenticated administrators can access all the additional device jobs:



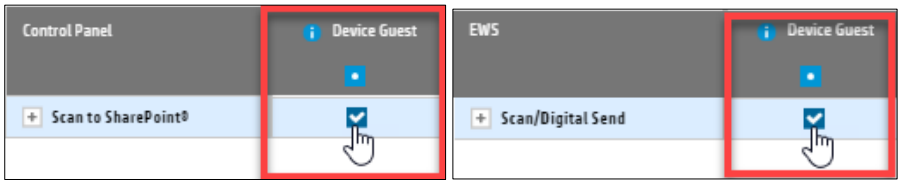
4. In the **Control Panel's Sign-In Method** column, select **PaperCut MF**:



5. In the **EWS's Sign-In Method** column, select **PaperCut MF**:



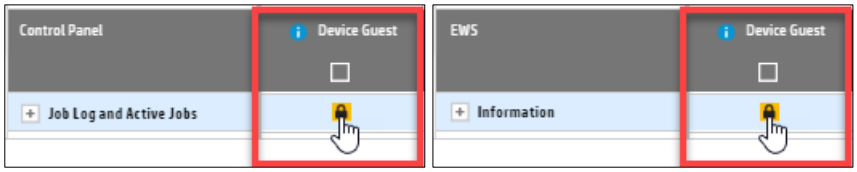
6. **Jobs that unauthenticated users can access:** In the required row(s) of the **Control Panel/ EWS**, ensure the **Device Guest** column's checkbox is **checked/ ticked:**



Note:

- Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.
- "Quota service error").
- This overrides any existing **Filters and Restrictions** that may be configured in the PaperCut MF Admin web interface for the device's printer.
  For example, if the device's Printer (**Printers > Printer List > Printer Details > Filters & Restrictions** page) has **Groups With Color Access** > **Only allow the following groups to print in color** set to a specific group of users, but if the **Device Guest** column is enabled with **Print in color**, then all users can print in color.
- This alters the device's first screen and the resulting login workflow on devices running **HP FutureSmart 4 Firmware Bundle Version** is **4.5.5 or above**. For more information, see 6.4 Device's first screen and login workflow.
- To ensure the device's paper trays are configurable, ensure the **Ability to modify tray size and type settings** is **checked/ ticked**, and not **Locked**. For more information, see 6.11 Paper trays are not configurable.

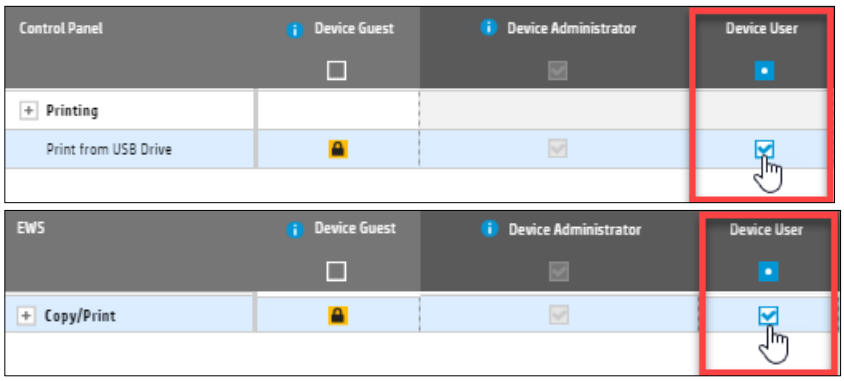
7. **Jobs that only authenticated, non-administrative users can access:** In the required row(s) of the **Control Panel/ EWS**:
   i. ensure the **Device Guest** column's checkbox is **Locked:**



Note:

- Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.
  "Quota service error").
- To ensure the device's paper trays are configurable, ensure the **Ability to modify tray size and type settings** is **checked/ ticked**, and not **Locked**. For more information, see 6.11 Paper trays are not configurable.

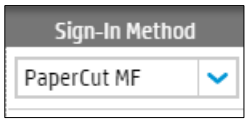
ii. ensure the **Device User** column's checkbox is **checked/ ticked:**



Note:

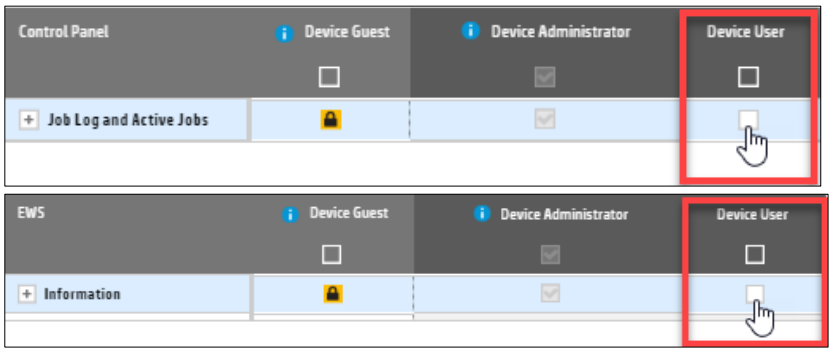
- Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.
  "Quota service error").

iii. ensure the **Sign-In Method** column's dropdown is either **PaperCut MF** or **Use Default**:



8. **Jobs that only authenticated administrators can access (i.e. non-administrative users cannot access):** In the required row(s) of the **Control Panel/ EWS**:

i. ensure the **Device User** column's checkbox is **unchecked/ unticked:**

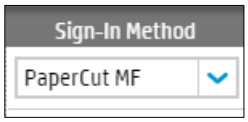


Note:

- These jobs appear "locked" to non-administrative users. Only authenticated administrators can access them. Only authenticated administrators can access them. For more information, see 6.10 Accessing "locked" administrative jobs.
- Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore`

command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.
"Quota service error").

ii. ensure the **Sign-In Method** column's dropdown is either **PaperCut MF** or **Use Default**.



9. Click **Apply**.

4.7.2 User selection of an account

If tracked device jobs (such as, on-device print jobs) 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 toggle the display of the PaperCut MF **Account Selection** icon on the device's Home screen, use the config key **ext-device.hp-oxpd.register.account-selection.** For more information, see 4.13 Config Editor.

- To configure the PaperCut MF Account Selection screen, use the config key **ext-device.hp-oxpd.account-list.limit**. For more information, see 4.13 Config Editor.

4.7.3 Job costs and account balances

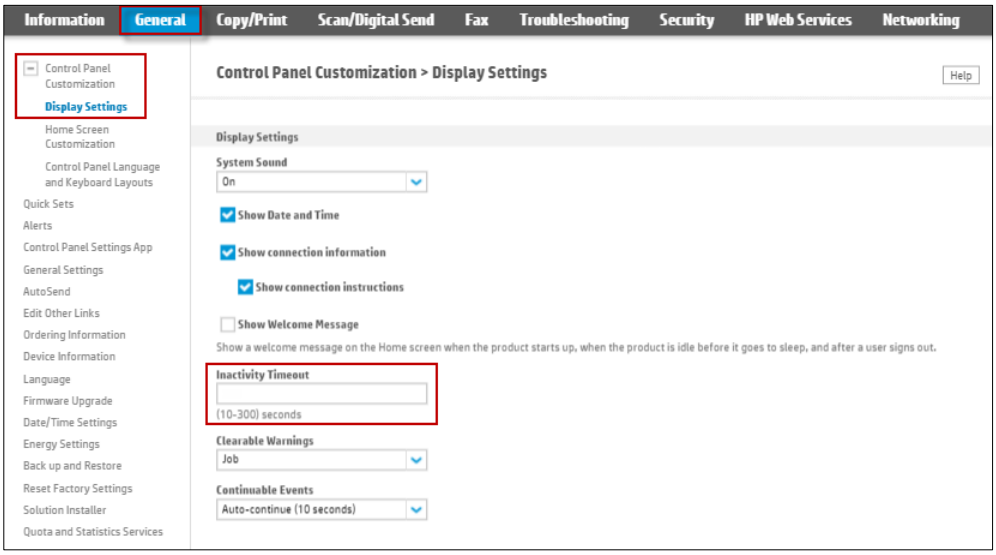
When printing, if a restricted user's account balance is insufficient to cover the cost of the restricted user's entire print job, PaperCut MF prevents the user from being able to start the print job. This ensures that the restricted user's account balance never drops below zero for print jobs.

However, when using the device to print from a USB or storage device, a restricted user's account balance can drop below zero. You can minimize this by using the config key **ext-device.hp-oxpd.restricted.multiple-txns** to prevent restricted users from being able to perform multiple transactions simultaneously on the device. For more information, see 4.13 Config Editor.

4.8 Timeouts

A logged-in user who is detected as being idle (on a PaperCut MF screen or a non-PaperCut MF device screen) is automatically logged out after a certain interval of time, based on the following conditions:

- **Device's timeout** - If the logged-in user is idle on a non-PaperCut MF device screen, then the user is logged out based on the device's timeout.
  To configure the device's timeout:
  a. Log in to the device's web interface as an administrator.
  b. Navigate to **General > Control Panel Customization > Display Settings.**
  c. In **Inactivity Timeout**, enter the required device timeout.



Note: If the logged-in user is idle on a non-PaperCut MF device screen, then the user is logged out based on this value. However, if the logged-in user is idle on a PaperCut MF screen and if this value is lower than the PaperCut MF timeout (the config key **ext-device.inactivity-timeout-secs**), then the user is logged out based on this value (i.e. this value supersedes and overrides the higher value of the config key). For more information, see 4.8 Timeouts and 4.13 Config Editor.

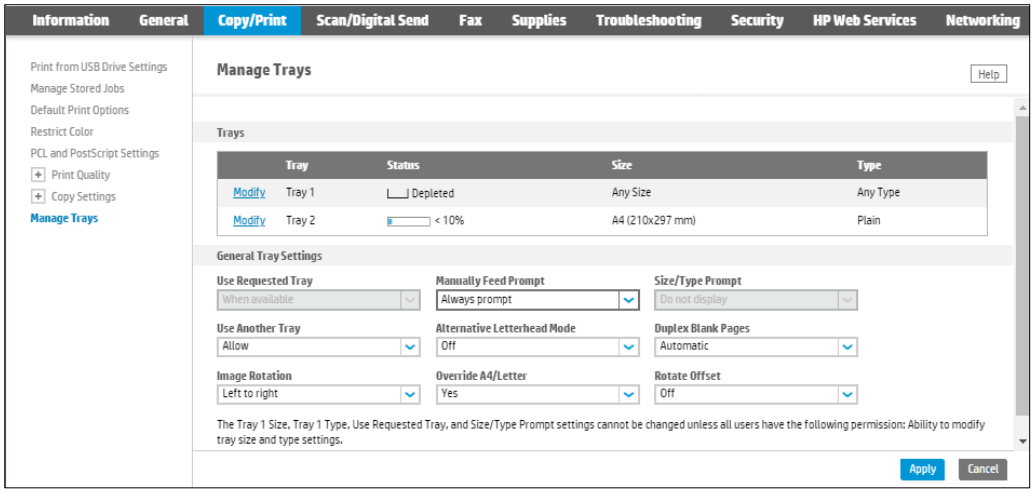
  d. Click **Apply**.
- **PaperCut MF's timeout** - If the logged-in user is idle on a PaperCut MF screen, then the user is logged out based on the config key **ext-device.inactivity-timeout-secs** or the device's timeout, whichever has the lower value. For more information, see 4.13 Config Editor.

4.9 Device's Manage Trays settings

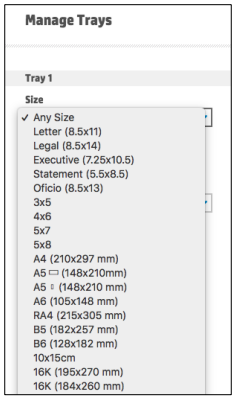
To configure the device's Manage Trays settings:

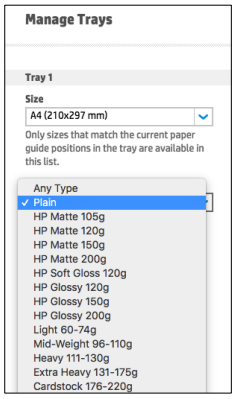
1. Log in to the device's web interface as an administrator.

2. Navigate to **Copy/Print > Manage Trays**:



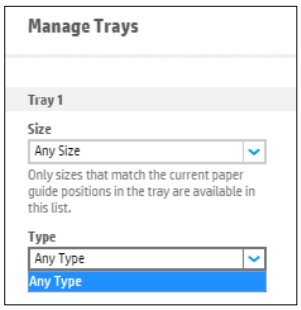
3. In **Trays**, click **Modify** for the required tray you are modifying.
4. In **Size** and **Type**, select the required paper size and type for this tray:





5. Click **Apply**.

   Note: If the **Size** and **Type** fields do not display required dropdown options, then see 6.11 Paper trays are not configurable.



4.10 Device's Control Panel Language and Keyboard Layouts settings

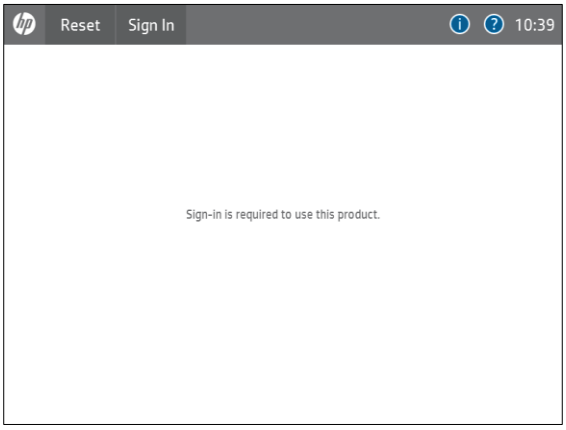
To configure the device's Control Panel Language and Keyboard Layouts settings:

1. Log in to the device's web interface as an administrator.
2. Navigate to **General > Control Panel Customization > Control Panel Language and Keyboard Layouts.**
3. Set the **Control Panel Language and Keyboard Layouts** fields as required.
4. Click **Apply**.

4.11 Device's first screen's message

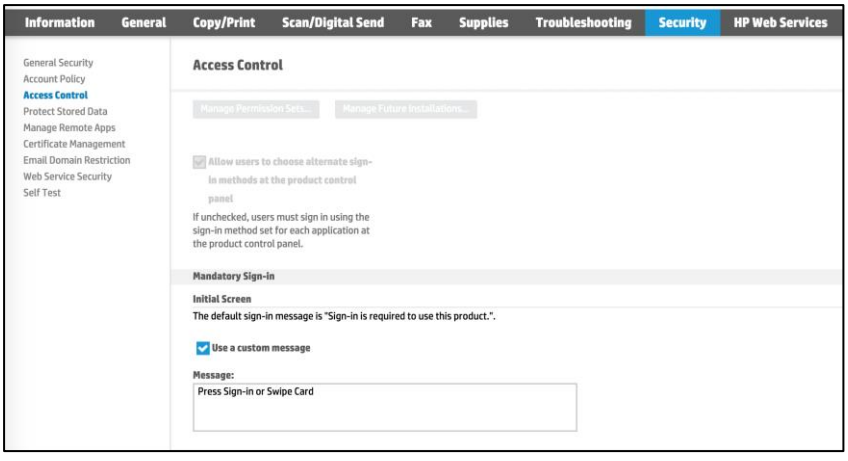
Note: This is only applicable to devices running **HP FutureSmart 4 Firmware Bundle Version 4.5.5 or above**. For more information, see 6.4 Device's first screen and login workflow.

The first screen on devices running **HP FutureSmart 4 Firmware Bundle Version 4.5.5 or above**, is usually a white screen with the following default message, which you can customize:



To customize the device's first screen message:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Access Control.**
3. In **Mandatory Sign-In > Initial Screen**, select **Use a custom message**.
4. In **Message**, enter the required text.
   For example, instructions to help users access the device.



5. Click **Apply.**

4.12 Screen headers

4.12.1 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.hp-oxpd.header.color
   ext-device.hp-oxpd.header.textcolor
   For more information, see 4.13 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.

4.12.2 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 = 28 pixels
   - Image width = 58 pixels
   - Image file size = less than 20kB
   - Image file format = `.png`
   - Image filename = `logo.png` or `small-logo.png`
   - Image file location = `[PaperCut Install Location]\server\custom\web\device\hp-oxp\`
2. Log in to the device as a test user (simple test user).
3. Verify that the device's header logo is as required.

4.13 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.hp-oxpd.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 • Default: DEFAULT (device-specific PaperCut MF text) **Note:** To add a line break, use *\n.* For example, *PaperCut Software\nSwipe your card to log in*.
ext-device.hp-oxpd.login.id-field.numeric	Toggle whether the login ID field contains only numbers. When enabled a soft number pad is displayed in place of the soft keyboard. This is a device-specific config key. • Values: Y, N, DEFAULT • Default: DEFAULT (N) **Note:** Some device/firmware combinations may not have this feature, and will display the soft keyboard instead.
ext-device.hp-oxpd.header.color	Customize the background color of headers on all PaperCut MF screens. This is a device-specific config key. • Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT (dark green) **Note:** For more information, see 4.12.1 Header colors.
ext-device.hp-oxpd.header.textcolor	Customize the text color of headers on all PaperCut MF screens. This is a device-specific config key.

	• Values: #RRGGBB (hexadecimal web/ HTML notation of Red:Green:Blue), DEFAULT • Default: DEFAULT (white) **Note:** For more information, see 4.12.1 Header colors.
ext-device.hp-oxpd.release-show-cost	Toggle the display of the cost of held print jobs on the PaperCut MF Print Release and Print Settings screens. This is a device-specific config key. • Values: Y, N • Default: Y
ext-device.hp-oxpd.register.account-selection	Toggle the display of the **PaperCut MF Account Selection** icon on the device' Home screen. This is a device-specific config key. • Values: Y, N • Default: Y **Note:** For more information, see 4.7.2 User selection of an account.
ext-device.hp-oxpd.account-list.limit	Specify the maximum number of applicable shared accounts displayed on the PaperCut MF Account Selection screen. This is a device-specific config key. • Values: 1-500 • Default: 100 **Note:** For more information, see 4.7.2 User selection of an account.
ext-device.hp-oxpd.permission.server-managed	Configure access permissions for the additional device jobs using: • PaperCut MF, or • the device's web interface This is a device-specific config key. • Values: Y (configure access permissions using PaperCut MF), N (configure access permissions using device's web interface)

	• Default: Y
	
	Note:
	
	• Setting this to Y –
	  ○ uses PaperCut MF to configure access permissions for the additional device jobs.
	  ○ requires PaperCut MF's config keys **ext-device.hp-oxpd.permission.whitelist** and **ext-device.hp-oxpd.guest.permission.whitelist** to be configured.
	  ○ overrides access permissions configured on the device's web interface.
	• Setting this to N –
	  ○ uses the device's web interface to configure access permissions for the additional device jobs.
	  ○ requires the device's web interface's Access Control settings to be configured.
	  ○ overrides access permissions configured via PaperCut MF's config keys **ext-device.hp-oxpd.permission.whitelist** and **ext-device.hp-oxpd.guest.permission.whitelist**
	• For more information, see 4.7.1.1 Additional device jobs.

ext-device.hp-oxpd.permission.whitelist	Specify the additional device jobs that only authenticated users can access.
	
	This is a device-specific config key.
	
	• Values: * (all the following additional device jobs), any one or a comma-separated combination of the following additional device jobs (not case sensitive):
	  ○ Copy
	  ○ Copy/Print
	  ○ Scan
	  ○ USB Drive
	  ○ Network Folder
	  ○ Email
	  ○ Scan to USB Drive

    - Scan to Job Storage
    - Scan to Network Folder
    - Scan to SharePoint®
    - Print from Job Storage
    - Print from USB Drive
    - Print in color
    - Scan/Digital Send
    - Ability to edit the network folder path
    - Load Scan to Network Folder Quick Set
    - Load Scan to USB Drive Quick Set
    - 1-sided copy output
    - Make a Color Copy
    - Load Copy Quick Set
    - Fax
    - Load Fax Quick Set
    - Ability to edit the From field for email
    - Ability to edit the To field for email
    - Ability to edit the CC field for email
    - Ability to edit the BCC field for email
    - Ability to edit the Subject field for email
    - Ability to edit the body of an email
    - Load Email Quick Set
- Default: * (all the above additional device jobs)

Note:

- This is only applicable if the config key **ext-device.hp-oxpd.permission.server-managed** is set to Y.
- This is not an exhaustive list of all the additional device jobs. For more information, see the log file located in: `[PaperCut MF Install Location]\server\logs\hp-oxp-installed-apps.log`
- Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the

	certificate is valid. Refer to the PaperCut MF manual for more details. • "Quota service error"). • To ensure the device's paper trays are configurable, do not include the value **Ability to modify tray size and type setting**s. For more information, see 4.9 Device's Manage Trays settings and 6.11 Paper trays are not configurable.
ext-device.hp-oxpd.guest.permission.whitelist	Specify the additional device jobs that unauthenticated users can access. This is a device-specific config key. • Values: any one or a comma-separated combination of the additional device jobs (not case sensitive) listed in the log file located in: `[PaperCut MF Install Location]\server\logs\hp-oxp-installed-apps.log` **Note:** • This is only applicable if the config key ext-device.hp-oxpd.permission.server-managed is set to Y. • Ensure this does not contradict the settings configured on the PaperCut MF Admin web interface (see 4.7.1 Tracking device jobs). If there is a contradiction, the device displays the **Quota service error** (see 0 On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details. • "Quota service error"). • This alters the device's first screen and the resulting login workflow on devices running **HP FutureSmart 4 Firmware Bundle Version** is **4.5.5 or above**. For more information, see 6.4 Device's first screen and login workflow.

	• To ensure the device's paper trays are configurable, include the value **Ability to modify tray size and type settings**. For more information, see 4.9 Device's Manage Trays settings and 6.11 Paper trays are not configurable.
"Swipe card" authentication option	

ext-device.hp-oxpd.fast-swipe-login-flow	Enable or disable quick swipe-to-login.
	
	This is a device-specific config key.
	
	• Values: Y (quick swipe-to-login), N (standard swipe-to-login), DEFAULT
	• Default: DEFAULT (N)
	
	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 User authentication via swipe cards.
	• Setting this to Y –
	  ○ enables quick swipe-to-login
	  ○ could also cause some issues, based on the device's **HP FutureSmart 4 Firmware Bundle Version**. For more information about compatible versions, see the Known Issues with HP (PaperCut MF) page.

ext-device.hp-oxpd.skip-hid-restart	Specify whether or not the device skips the HID restart when a user logs in with a swipe card. This is a device-specific config key. • Values: Y, N • Default: DEFAULT (N) **Note**: • Setting this to Y – Enables skipping the HID restart during card swiping. The login time might be reduced to approximately 3-6 seconds. • Setting this to N – Disables skipping the HID restart during card swiping.

ext-device.hp-oxpd.register.card-reader	Specify whether or not PaperCut MF is allowed to automatically register and establish an exclusive lock on card readers that are detected on the device. This is a device-specific config key. • Values: Y, N • Default: Y **Note:** • Setting this to Y – only allows PaperCut MF to exclusively use card readers, preventing third-party applications from using them. This is only recommended if the **Swipe card** authentication option is selected. For more information, see 4.3 User authentication options and 4.4 User authentication via swipe cards • Setting this to N – allows third-party applications to use card readers. This is recommended if card readers are not used by PaperCut MF for swipe card authentication.
ext-device.hp-oxpd.additional-card-readers.vid-pid.hex	Specify the card readers that are supported by PaperCut MF, in addition to the list of already supported card readers. This is a device-specific config key. • Values: any one or a comma-separated list of *0xVID:0xPID* of card readers (hexadecimal web/ HTML notation). For example, for the *Bio-Buddy Converter*, specify *0x2f9f:0x0110*. **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 User authentication via swipe cards, 4.4.1 Supported card readers.
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 4.3 User authentication options
ext-device.self-association-allowed-card-regex	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 4.3 User authentication options and 4.4.3 Handling card identifiers
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.
ext-device.card-no-converter	Specify the converters (standard format converters, custom JavaScript converters, or both) to be used to modify card identifiers for authentication This is a global and device-specific config key. Device-specific: • Values: Any valid converter (standard format converters, custom JavaScript converters, or both), GLOBAL (inherited from global settings) • Default: GLOBAL (inherited from global settings) Global: • Values: Any valid converter (standard format converters, custom JavaScript converters, or both) **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.
Job costs and account balances	
ext-device.hp-oxpd.restricted.multiple-txns	Specify whether or not restricted users are permitted to perform multiple transactions simultaneously on the device. This is a device-specific config key. • Values: N (multiple transactions not permitted), Y (multiple transactions permitted) • Default: N **Note:** • This is only applicable to restricted users.

	• Setting this to N – is recommended to ensure that restricted users' account balances do not drop below zero. For more information, see 4.7.3 Job costs and account balances.
Network resilience, security, debug logs, uninstallation	
system.network-address	Specify the network IP address or FQDN (Fully Qualified Domain Name) of the PaperCut MF Application Server that the device uses to make inbound connections. This is a global config key. • Values: Network IP address or FQDN (Fully Qualified Domain Name) of the PaperCut MF Application Server used by the device for inbound connections. **Note:** For more information, see 4.1.1 Inbound connections to PaperCut MF Application Server.
ext-device.hp-oxpd.use-ssl	Toggle the use of the encrypted, secure HTTPS (SSL/TLS) protocol for communication between PaperCut MF and the device. This is a device-specific config key. • Values: N (TCP/HTTP), Y (SSL/TLS/HTTPS) • Default: N (TCP/HTTP) **Note:** Ensure to set the config key **ext-device.hp-oxpd.port-num** as required. For more information, see 4.2.1 HTTPS Security (recommended).
ext-device.hp-oxpd.port-num	Specify the port of the device to be used for communication between PaperCut MF and the device. This is a device-specific config key. • Values: 80 (TCP/HTTP), 443 (SSL/TLS/HTTPS), any other valid port number based on your networking/firewall configuration • Default: 80 (TCP/HTTP)

	Note: Ensure to set the config key **ext-device.hp-oxpd.use-ssl** as required. For more information, see 4.2.1 HTTPS Security (recommended).
ext-device.hp-oxpd.period.ping	Specify the interval of time (seconds) between each attempt made by PaperCut MF to connect to the device. This is a device-specific config key. • Values: 1-3600 (seconds) • Default: 300 (seconds)
ext-device.hp-oxpd.period.error	Specify the interval of time (seconds) between each attempt made by PaperCut MF to connect to the device, after encountering an error when installing PaperCut MF on the device (i.e. device registration and integration). This is a device-specific config key. • Values: 1-3600 (seconds) • Default: 60 (seconds)
ext-device.hp-oxpd.device-setup-complete.delay-secs	Specify the interval of ramp-up time (seconds) following device registration after which the device can be used. This is a device-specific config key. • Values: 0-20 (seconds) • Default: 5 (seconds) **Note:** Use this only if there is an open support ticket with PaperCut Support.

ext-device.block-release-on-error.snmp-error-list	Specify the errors that will prevent jobs from being released.
	
	This is a global config key.
	
	• Values: DEFAULT, any one or a comma-separated combination of the following printer error types (not case sensitive):
	  ○ lowPaper
	  ○ noPaper
	  ○ lowToner
	  ○ noToner
	  ○ doorOpen

	○ jammed ○ offline ○ serviceRequested ○ inputTrayMissing ○ outputTrayMissing ○ markerSupplyMissing ○ outputNearFull ○ outputFull ○ inputTrayEmpty ○ overduePreventMaint • Default: DEFAULT (noPaper, doorOpen, jammed, offline, inputTrayMissing, outputTrayMissing, markerSupplyMissing, outputFull)
ext-device.block-release-on-error.snmp-byte-order-mode	Specify the byte order used to notify PaperCut MF of printer errors. This is a global config key. • Values: FORWARD, REVERSE, DEFAULT • Default: DEFAULT (FORWARD) **Note:** • Setting this to DEFAULT – is recommended if you do not know the byte order used by the device. • Setting this to REVERSE – is recommended if SNMP notifications are incorrect.
Timeouts	
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) **Note:** This is only applicable if it is lower than the value of the device's timeout. However, if it is higher, then it is overridden by the lower value of device's timeout. For more information, see 4.8 Timeouts.
Enhanced user workflow	

ext-device.hp-oxpd.enhanced-mode	This is a global and device-specific config key. Global: • Values: Y, N, DEFAULT (currently N) • Default: DEFAULT **Note**: If you have a firmware that supports enhanced mode, and want a consistent experience across your fleet change the PaperCut MF global configuration key ext-device.hp-oxpd.enhanced-mode From DEFAULT to Y. DEFAULT behavior is off in 21.0. Device-specific: • Values: Y, N, GLOBAL • Default: GLOBAL (inherited from global settings) **Note:** • Setting this to Y or N overrides the Global Config key
ext-device.hp-oxpd.direct-to-release-page	This is a device-specific config key. Device-specific: • Values: Y, N • Default: N **Note:** Setting this to Y configures to login directly to print release.
ext-device.hp-oxpd.skip-release-screen-when-no-jobs	This is a device-specific config key. Device-specific: • Values: Y, N • Default: N **Note:** This key is relevant only if **ext-device.hp-oxpd.direct-to-release-page** is set to Y. Setting this also to Y, configures to login directly to print release, but to home screen if no jobs to release

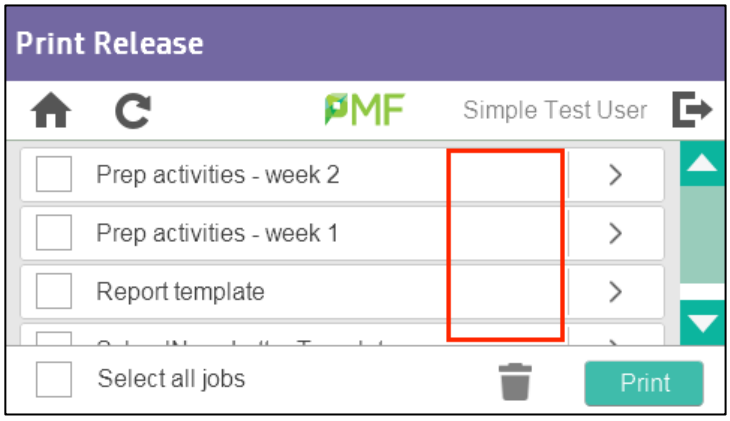
5 Known Limitations

5.1 Limitations with on-device printing

When using the device to print from a USB or storage device, a restricted user's account balance can drop below zero. This can be minimized by using the config key **ext-device.hp-oxpd.restricted.multiple-txns** to prevent restricted users from being able to perform multiple transactions simultaneously on the device. For more information, see 4.13 Config Editor.

5.2 Held print job timestamps are not displayed

The relative timestamps of held print jobs are not displayed on the PaperCut MF Print Release screen:



5.3 Guest access authentication is unavailable

Although anonymous access authentication is available, guest access authentication is currently unavailable. As a result, if the **Allow guest/anonymous access** authentication option is selected, all other options are automatically disabled, and cannot be used as authentication options on the device. For more information, see 4.3 User authentication options.

5.4 Some paper sizes are unsupported

Charges for some unsupported paper sizes cannot be configured on the device's **Device Details > Charging** page (they do not appear as an option in the **Add Size** field). As a result, the charge applied if using any of these paper sizes, is the default charge that is set on the **Device Details > Charging** page.

The list of unsupported paper sizes includes:

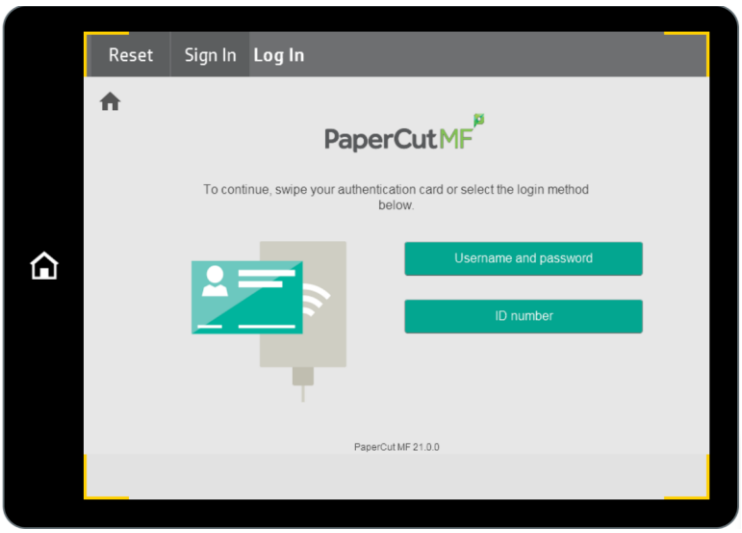
- Envelope_A2_4point375x5point75in
- Envelope_Catalog1_6x9in
- Envelope_Comm6point75_3point625x6point5in
- Envelope_Monarch_3point875x7point5in
- Envelope_Windsor_3point875x8point875in
- Invoice_5point5x8point5in
- JBusinessCard_55x91mm
- JDoublePostcard_148x200mm

- JDoublePostcard_Rotated_148x200mm
- JIS_Chou3_120x235mm
- JIS_Chou4_90x205mm
- JIS_Exec_216x330mm
- JIS_Kaku2_240x332mm
- JPostcard_100x148mm
- LongScan_8point5x34in
- Mutsugiri_203x254mm
- ISO_A_8_52_X_74_MM
- ISO_A_9_37_X_52_MM
- ISO_A_10_26_X_37_MM
- ISO_B_8_62_X_88_MM
- ISO_B_9_44_X_62_MM
- ISO_B_10_31_X_44_MM
- ISO_C_0_917_X_1297_MM
- ISO_C_1_648_X_917_MM
- ISO_C_2_458_X_648_MM
- ISO_C_7_81_X_114_MM
- ISO_C_8_57_X_81_MM
- ISO_C_9_40_X_57_MM
- ISO_C_10_28_X_40_MM
- JIS_B_0_1030_X_1456_MM
- JIS_B_6_128_X_182_MM
- JIS_B_7_91_X_128_MM
- JIS_B_8_64_X_91_MM
- JIS_B_9_45_X_64_MM
- JIS_B_10_32_X_45_MM
- DIN_2_A_0_1189_X_1682_MM
- DIN_4_A_0_1682_X_2378_MM
- ENVELOPE_DL_110_X_220_MM
- GENERAL_3_POINT_5_X_5_IN
- GENERAL_3_X_5_IN
- GENERAL_4_X_6_IN
- GENERAL_4_X_8_IN
- GENERAL_4_X_12_IN
- GENERAL_5_X_7_IN
- GENERAL_5_X_8_IN
- GENERAL_6_X_8_IN
- GENERAL_7_X_9_IN
- GENERAL_10_X_13_IN
- GENERAL_10_X_15_IN
- GENERAL_11_X_12_IN
- GENERAL_11_X_14_IN

- GENERAL_11_X_19_IN
- GENERAL_12_X_12_IN
- GENERAL_12_X_14_IN
- GENERAL_12_X_19_IN

5.5 In enhanced mode, pressing the 'Sign In' button before swiping an authentication card might cause unexpected behaviours

When a user uses an authentication card swipe to log in in enhanced mode, they should not (and do not need to) press the **Sign In** button before swiping the card.



Pressing the Sign In button could cause the following:

- If the card is not associated with any user, and card association is not enabled, the card swipe will fail without displaying any error message.
- If the card is not associated with any user, and card association is enabled, after swiping the card, the card association screen will not be displayed.
- If the card is associated with a user, and the card swipe requires PIN, after swiping the card, the enter PIN screen will not be displayed.

6 FAQ & Troubleshooting

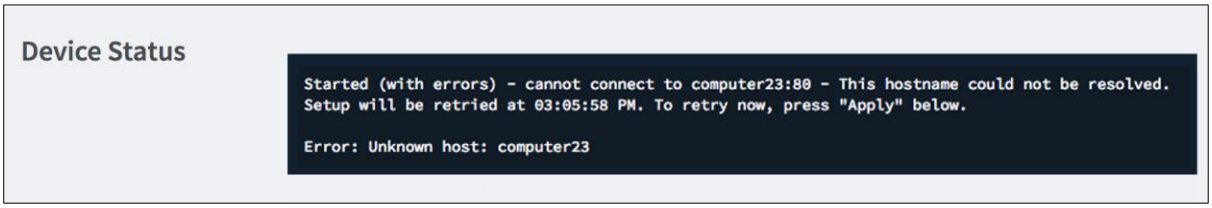
6.1 IP addresses of the PaperCut MF Application Server

To get the IP addresses of the PaperCut MF Application Server, run any one of the following applicable commands from the command line prompt:

- For Windows: `ipconfig`
- For Linux, Mac OS: `ifconfig`

6.2 Device Status "Started (with errors)"

After attempting to install PaperCut MF on the device, if the **Device Status** displays **Started (with errors)**, it implies that PaperCut MF installation is unsuccessful because there are errors in the **Create Device** fields (**Type, Device name, Hostname / IP, Device's administrator** credentials) or errors on the device or both.



To resolve this:

1. Address any device-specific errors outlined on the device.
2. Log in to the PaperCut MF Admin web interface.
3. Navigate to **Devices**.
4. Click the **Device Name** of the device displaying the error status in the **Status** column.
5. Resolve the error based on the cause and resolution as outlined in the **Device Status**.
6. Click **Apply**.

6.3 Device Status "Stopped (with errors)"

After attempting to install PaperCut MF on the device, if the **Device Status** displays **Stopped (with errors)**, it implies that PaperCut MF installation is unsuccessful:

This is because the device is not compatible with the embedded software solution specified in the **Type** field (i.e. **HP OXP (Printer Only)**). For more information, see 2 Installation.

6.4 Device's first screen and login workflow

After PaperCut MF is successfully installed on the device, the **HP FutureSmart 4 Firmware Bundle Version** of the device determines its first screen and the resulting login workflow and actions, which could be either:

- 6.4.1 Screen with icons
- 6.4.2 White screen with a message

6.4.1 Screen with icons

If the device's **HP FutureSmart 4 Firmware Bundle Version** is **below 4.5.5**, then the device displays a screen with the following icons:

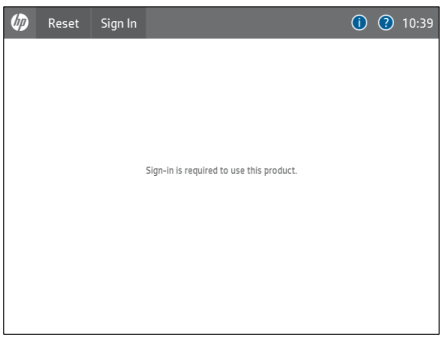
Clicking **Reset**, displays PaperCut MF icons:

Users can access the PaperCut MF Login screen by any of the following options:

- clicking **Sign In**,
- using their swipe cards (if the **Swipe card** authentication option is selected),
- clicking any other application on the device.

6.4.2 White screen with a message

If the device's **HP FutureSmart 4 Firmware Bundle Version** is **4.5.5 or above**, and it does not allow unauthenticated users to access device jobs, then the device displays a white screen with the following default message (to customize this message, see 4.11 Device's first screen's message):



Users can access the PaperCut MF Login screen by any of the following options:

- clicking **Sign In**,
- using their swipe cards (if the **Swipe card** authentication option is selected)

Note: However, if unauthenticated users are allowed to access device jobs, (see, 4.7.1.1 Additional device jobs) then, the device's first screen and the resulting login workflow and actions reverts to that of devices running **HP FutureSmart 4 Firmware Bundle Version below 4.5.5**. As a result, the device's first screen is a screen with the non-PaperCut MF icons, instead of the white screen with a message (see, 6.4.1 Screen with icons).

6.5 Swipe card authentication anomalies

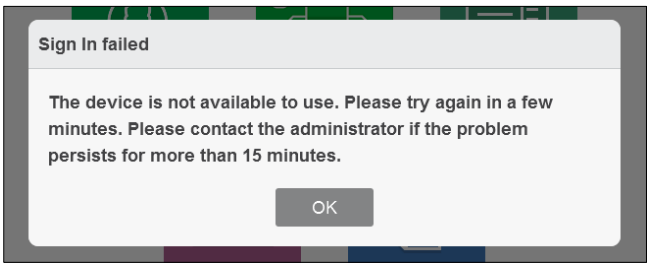
After PaperCut MF is successfully installed on the device, if swipe card authentication causes some problems during login or during card self-association, it implies that the card reader configuration on the PaperCut MF Admin web interface is incorrect.

To resolve this:

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's **Swipe card > Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)** ensure that if any one of the following card types is selected, then its conflicting other is not also selected as another card type:
   - ***Either*** HID Prox ***or*** HID Prox UID
   - ***Either*** MiFare CSN (Philips, NXP) ***or*** MiFare Ultralight CSN (Philips, NXP)
   - ***Either*** MiFare CSN (Philips, NXP) ***or*** iClass CSN, ISO1443A CSN, IS015693A (RDR-758x Compatible)

6.6 "Device is not available to use" error

After PaperCut MF is successfully installed on the device, if the device displays the following error when users attempt to log in, it implies that incorrect modifications have been made to the device's settings on the **Devices > External Device List > Device Details** page:



To resolve this:

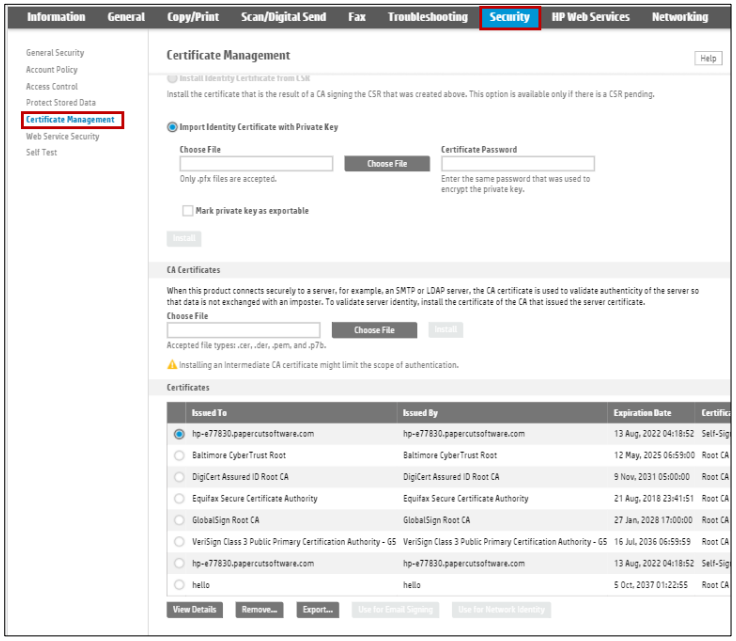
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Click the **Device Name** of the device displaying the error status in the **Status** column.
4. Resolve the error based on the cause and resolution as outlined in the **Device Status** area.
5. Click **Apply**.

6.7 Device Status "Started (with errors) – Certificate error"

After attempting to enable HTTPS, if the **Device Status** displays **Started (with errors) – Certificate error**, it implies that the limited number of certificates allowed on the device has been exceeded:

To resolve this:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Certificate Management**:



3. Delete any unused certificates.
4. Log in to the PaperCut MF Admin web interface.
5. Navigate to **Devices**.
6. Select the required device.
7. Click **Apply**.

6.8 The device is unable to connect to the PaperCut MF Application Server using HTTPS (SSL/TLS)

If the device is unable to connect to the PaperCut MF Application Server using HTTPS (SSL/TLS), it is because there are errors in the HTTPS configuration. To resolve this, ensure the following are configured appropriately:

- 6.8.1 Config keys
- 6.8.2 FQDN (or IP Address)
- 6.8.3 Root and Intermediary Certificates for CA-signed SSL certificates

6.8.1 Config keys

- Ensure the config key **ext-device.hp-oxpd.use-ssl** is set to **Y**. For more information, see 6.8.1 Config keys.
- It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 6.8.1 Config keys.

6.8.2 FQDN (or IP Address)

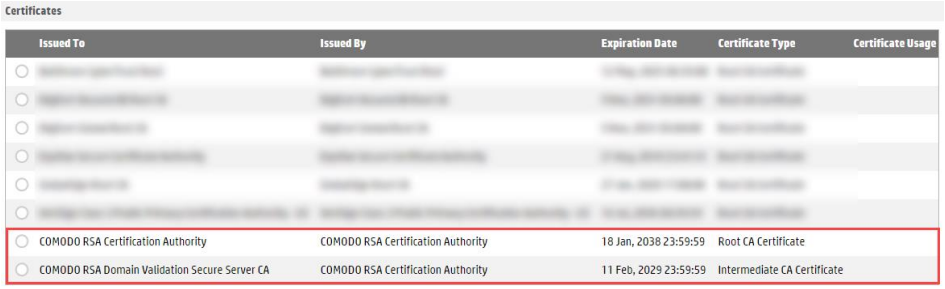
Ensure that the Fully Qualified Domain Name (or IP address) is the same in each of the following:

- the value of the PaperCut MF config key **system.network-address**
- the `<SYSTEM-NAME>` parameter used in the `create-ssl-keystore` command when either re-generating the PaperCut MF self-signed SSL certificate or when importing an official CA-signed, trusted SSL certificate into the PaperCut MF keystore
- the **Quota Server URL** in the device's web interface (**General > Quota and Statistics Services**)

6.8.3 Root and Intermediary Certificates for CA-signed SSL certificates

If using a CA-signed SSL certificate, ensure that the relevant Root and any required Intermediary Certificates are installed and listed on the device's web interface:

1. Log in to the device's web interface as an administrator.
2. Navigate to **Security > Certificate Management**.
3. In the **CA Certificates > Certificates** table, verify that the relevant Root and any required Intermediary Certificates are listed.
   For example:



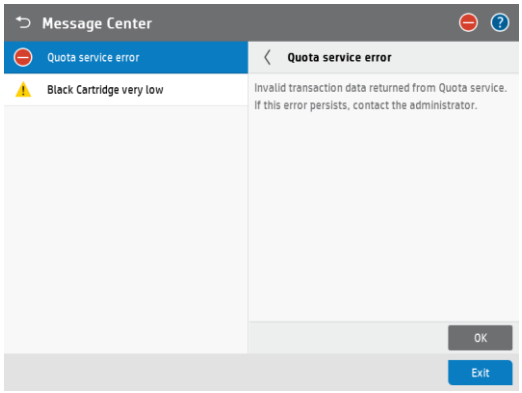
   Note:
   - If the relevant Root Certificate is not listed, click **Choose File**; select the relevant Root Certificate, click **Open**, and then click **Install**.
   - If the relevant Intermediary Certificate is not listed, click **Choose File**; select the relevant Intermediary Certificate, click **Open**, and then click **Install**.

6.8.4 Self-signed SSL certificates

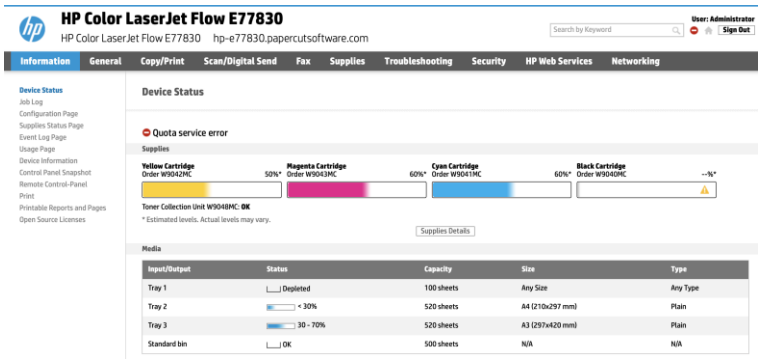
On newer HP Gemstone devices, it may be required for self-signed certificates to include a country code. The Country (C) key of the `RDN` parameter in the `create-ssl-keystore` command can be used to set the country code and ensure that the certificate is valid. Refer to the PaperCut MF manual for more details.

6.9 "Quota service error"

After PaperCut MF is successfully installed on the device, if the device displays the following error when users attempt to access device jobs, it implies that there are contractions in the configured settings (see 4.7.1 Tracking device jobs and 4.7.1.1 Additional device jobs):



The device's web interface also displays a similar error:

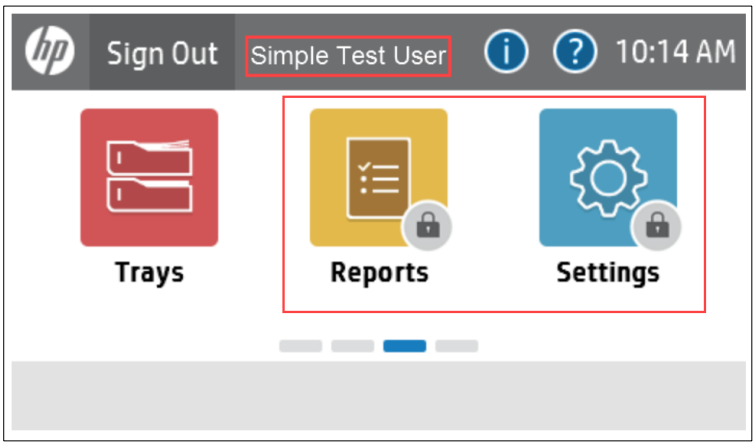


This prevents users from being able to use the device jobs that have contradicting configurations.

To resolve this, ensure that there are no contractions in the configured settings.

6.10 Accessing "locked" administrative jobs

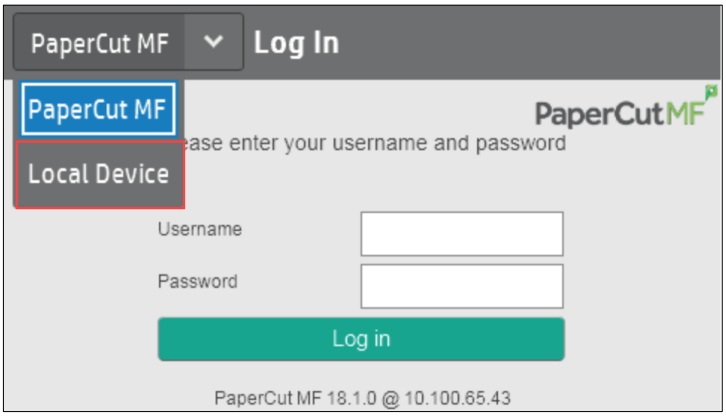
By default, PaperCut MF "locks" certain device jobs (such as, Supplies, Contacts, Reports, Settings, Support Tools, Job Log). They appear "locked" to non-administrative users (such as, the simple test user). Only authenticated administrators can access them.



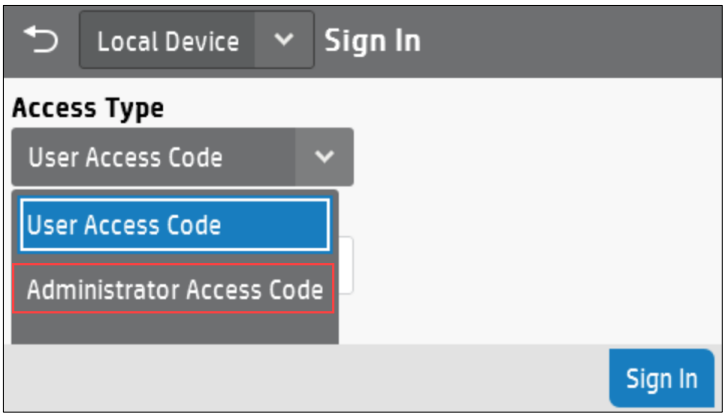
Note: For more information about configuring access permissions for required device jobs, see 4.7.1.1 Additional device jobs.

To access "locked" administrative jobs:

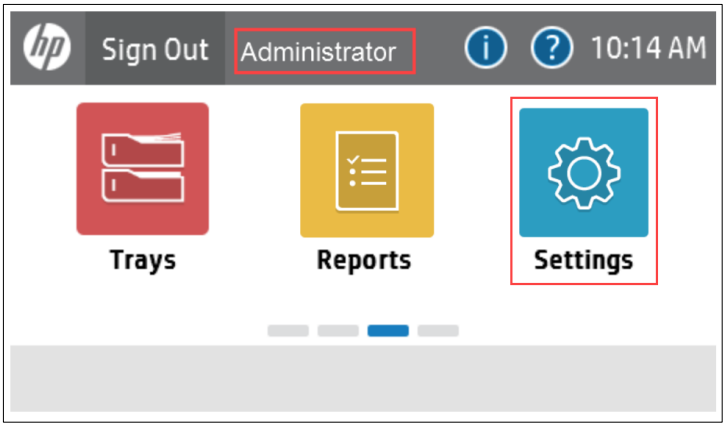
1. Navigate to the PaperCut MF Login screen on the device.
2. Select **Local Device**:



3. Select **Administrator Access Code**:



4. In **Access Code**, enter the administrator credentials (password) used for the device's web interface. For more information, see 2.4.1 Log in to the device's web interface as an administrator.
5. Click **Sign In**.
6. Select the required job (such as, Supplies):



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

6.11 Paper trays are not configurable

If the device's paper trays are not configurable, it is because unauthenticated users have been prevented from accessing the device job **Ability to modify tray size and type setting**:

- Either, on the PaperCut MF Admin web interface, the **Ability to modify tray size and type setting** is not a value of the config key **ext-device.hp-oxpd.guest.permission.whitelist,** or it is a value of the config key **ext-device.hp-oxpd.permission.whitelist**,
- Or, on the device's web interface, the **Control Panel's Ability to modify tray size and type settings** checkbox of the **Device Guest** column is **Locked**.

For more information, see 4.7.1.1 Additional device jobs.

To resolve this, use any one of the following options:

- 6.11.1 Using PaperCut MF
- 6.11.2 Using the device's web interface

6.11.1 Using PaperCut MF

To resolve this using PaperCut MF, ensure that the config key:

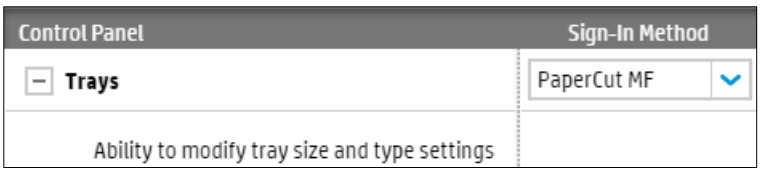
1. **ext-device.hp-oxpd.permission.server-managed** is set to ***Y***.
2. **ext-device.hp-oxpd.guest.permission.whitelist** contains the value ***Ability to modify tray size and type settings***.
3. **ext-device.hp-oxpd.permission.whitelist** does not contain the value ***Ability to modify tray size and type settings***.

For more information, see 4.13 Config Editor.

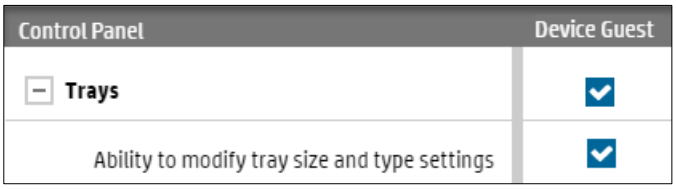
6.11.2 Using the device's web interface

To resolve this using the device's web interface:

1. Ensure that the config key **ext-device.hp-oxpd.permission.server-managed** is set to ***N***. For more information, see 4.13 Config Editor.
2. Log in to the device's web interface as an administrator.
3. Navigate to **Security > Access Control > Sign-In and Permission Policies.**
4. In the **Control Panel > Trays':**
   a. **Sign-In Method** column, select **PaperCut MF**:



   b. **Device Guest** column, ensure the checkboxes are **checked/ ticked**, and not **Locked**:



5. Click **Apply**.

6.12 Third-party applications are unable to use card readers

PaperCut MF automatically registers and establishes an exclusive lock on card readers that are detected on the device. As a result, they cannot be used by any other third-party applications. If the **Swipe card** authentication option is not selected (PaperCut MF is not being used for swipe card authentication), but third-party applications require access to card readers, then ensure to set the config key **ext-device.hp-oxpd.register.card-reader** to **Y**. For more information, see 4.13 Config Editor.

6.13 Can I improve the time it takes between swiping a card and logging in?

Yes. To reduce the login time, PaperCut recommends you set the following config keys:

- **ext-device.hp-oxpd.fast-swipe-login-flow=Y**
- **ext-device.hp-oxpd.skip-hid-restart=Y**

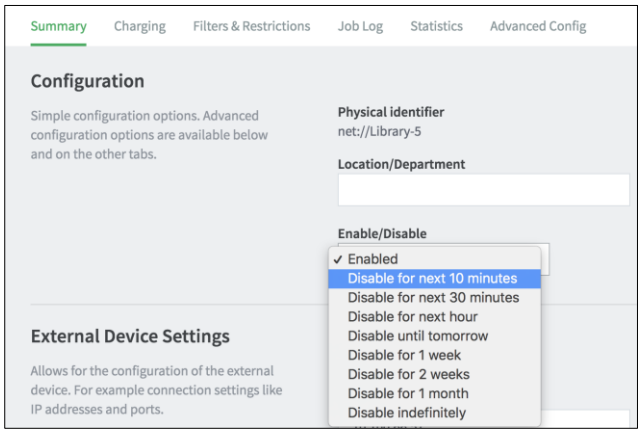
For more information, please refer to **4.4 User authentication via swipe cards.**

7 Uninstall *PaperCut MF - HP OXP Printer Only*

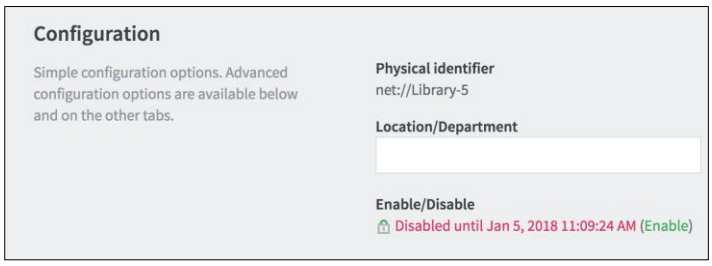
7.1 Temporarily disable *PaperCut MF - HP OXP Printer Only*

To temporarily disable *PaperCut MF - HP OXP Printer Only*:

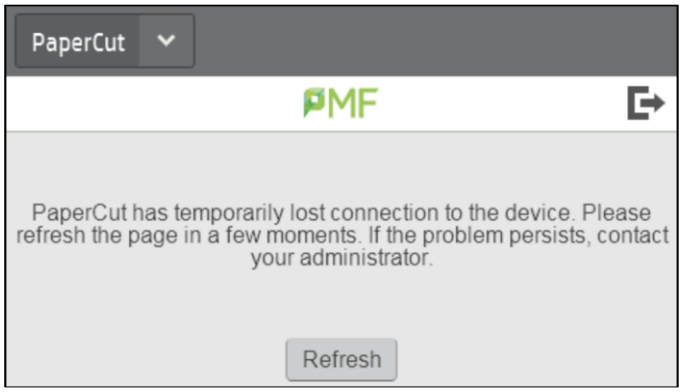
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the required device.
4. In the **Configuration** area's **Enable/Disable**, select a **Disable** option:



5. Verify that *PaperCut MF - HP OXP Printer Only* is disabled:



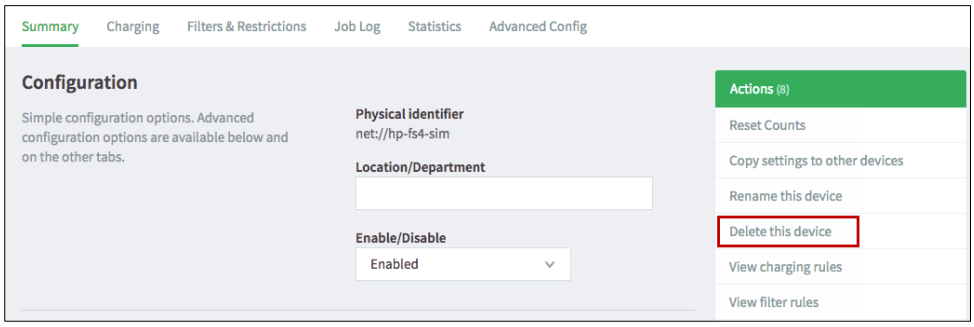
6. Verify that *PaperCut MF - HP OXP Printer Only* is not available on the device to users:



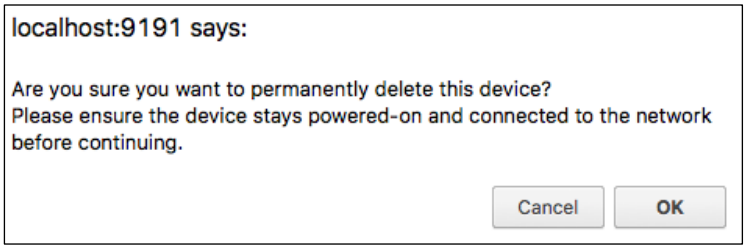
7.2 Permanently uninstall *PaperCut MF - HP OXP Printer Only*

To permanently uninstall *PaperCut MF - HP OXP Printer Only*:

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**:



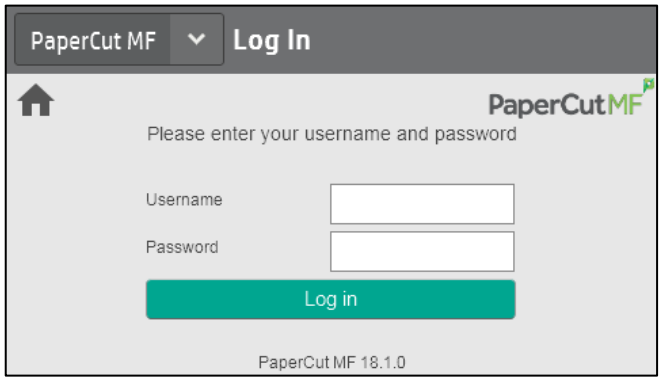
5. Click **Ok:**



6. Click **Devices** and verify that the device is no longer listed (*PaperCut MF - HP OXP Printer Only* is permanently uninstalled).
7. Verify that *PaperCut MF - HP OXP Printer Only* is not available on the device to users:

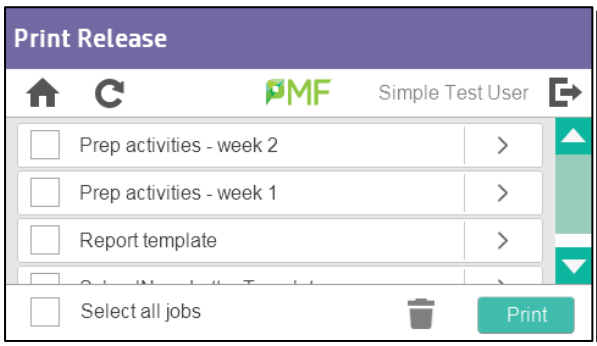
8 Appendix A: Device screens

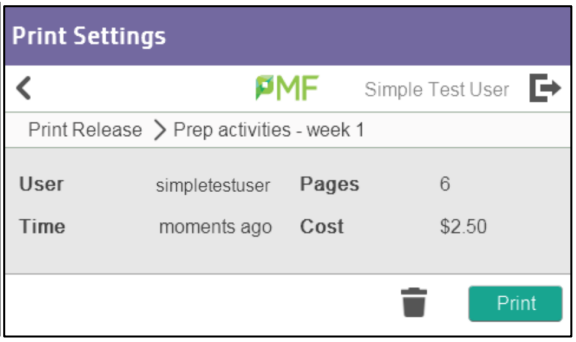
User authentication:



Home:

Secure Print Release:





Charging of jobs: