PaperCut MF - HP Pro (Fast Release) Embedded Manual

Contents

1 Version history

PaperCut MF version or date	Details
18.3.6	5.2 Security settings; 5.2 Security settings; 5.4 Config Editor; 8.6 The HTTPS (SSL/TLS) setup does not work
18.3.2	5.4 Config Editor
18.2.6	5.2 Security settings
18.2.4	5.3 "Swipe card" authentication method; 5.4 Config Editor
18.2.0	3 Installation; 8 FAQ & Troubleshooting
18.1.3	3.4.1 Install PaperCut MF; 6.4 Only the IPv4 format of the device’s IP address is accepted; 8.3 Device Status "Stopped (with errors)"
18.1.1	3.1 Supported devices; 3.2 System, access, and device requirements; 3.3 Setup procedures on the device web interface; 5.2.1 HTTPS Security; 5.3 "Swipe card" authentication method; 6 Known Limitations; 7 Uninstall *PaperCut MF - HP Pro (Fast Release);* 8 FAQ & Troubleshooting; 10 Appendix B: HP OXP Professional Services (OPS) server
18.1.0	New guide

2 Overview

This manual covers PaperCut's embedded software solution, *PaperCut MF - HP Pro (Fast Release)*, for compatible HP Pro devices. For general PaperCut MF documentation, see the PaperCut MF manual.

Some of the features of *PaperCut MF - HP Pro (Fast Release)* include:

- Secure access to the device via swipe card authentication (swipe to log in)
- Print release of held print jobs on successful authentication (Secure & Find Me Printing)
- Monitoring and tracking of printing (Charging and Logging)

Highlights of the embedded solution include:

2.1 Consistency

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

2.2 Integration

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

2.3 Rate of development

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

2.4 Vendor Neutral

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

2.5 Security

All embedded solutions are developed with both network and application security in mind, offering features like Secure & Find Me Printing, as well as use of SSL network protocols.

3 Installation

This section covers the installation of *PaperCut MF - HP Pro (Fast Release).*

3.1 Supported devices

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

3.2 System, access, and device requirements

Ensure that the following system, access, and device requirements are met:

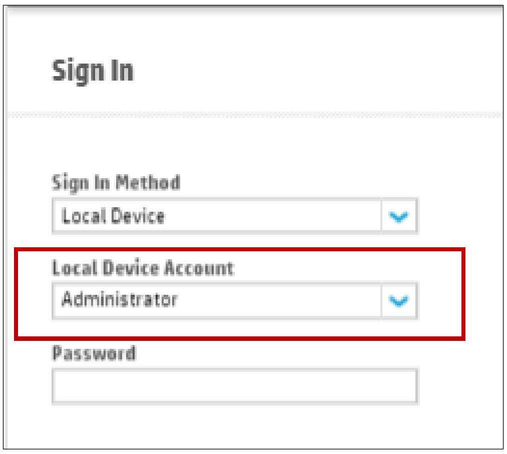
- The following entities are available:
    - Physical device – Administrator and user access, and credentials
    - Device's web interface – Administrator access, URL, and credentials
    - PaperCut MF Admin web interface – Administrator access, URL, and credentials
- The supported HP Pro devices on the network are compatible with PaperCut's embedded software solution, *PaperCut MF - HP Pro (Fast Release).*
- The supported HP Pro devices on the network have the HP OXP Professional Services (OPS) server installed. For more information, see 9 Appendix A: HP OXP Professional Services (OPS) server.
- The latest version of PaperCut MF is installed and running on the network. For more information, see the PaperCut MF manual.
  Note: The minimum compatible version is 18.1.0.
- The networking/firewall configuration allows:
    - Inbound connections to the PaperCut MF Application Server from the devices on the configured ports. For example:
        - 9191 (TCP/HTTP)
        - 9192 (SSL/TLS/HTTPS)
    - Outbound connections from the PaperCut MF Application Server to the devices on the configured ports. For example:
        - 80 (TCP/HTTP)
        - 443 (SSL/TLS/HTTPS)

3.3 Setup procedures on the device web interface

3.3.1 Log in to the device web interface

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**:



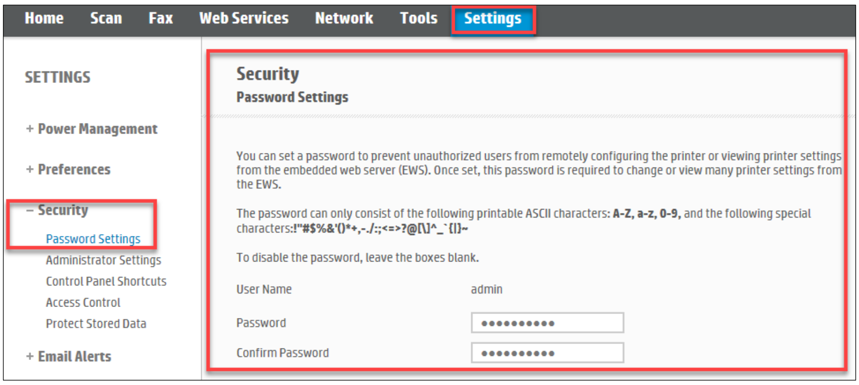
Sign In

Sign In Method: Local Device

Local Device Account: Administrator

Password

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 **Settings > Security > Password Settings**.
   d. Set the administrator credentials:



Security

Password Settings

You can set a password to prevent unauthorized users from remotely configuring the printer or viewing printer settings from the embedded web server (EWS). Once set, this password is required to change or view many printer settings from the EWS.

The password can only consist of the following printable ASCII characters: **A-Z, a-z, 0-9,** and the following special characters:**!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~**

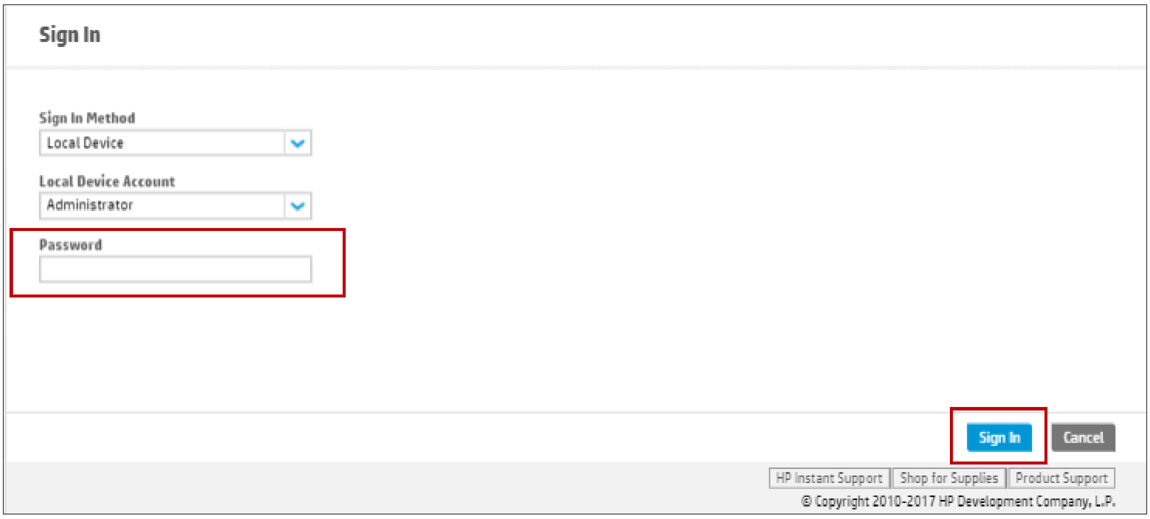
To disable the password, leave the boxes blank.

User Name: admin

Password: ●●●●●●●●●●

Confirm Password: ●●●●●●●●●●

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



Sign In

Sign In Method: Local Device

Local Device Account: Administrator

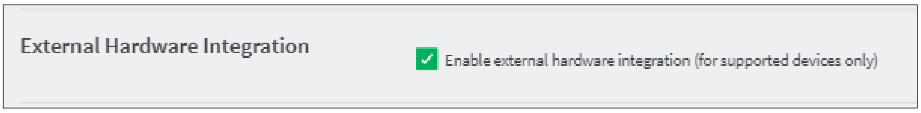
Password

3.4 Setup procedures on the PaperCut MF Admin web interface

3.4.1 Install PaperCut MF

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

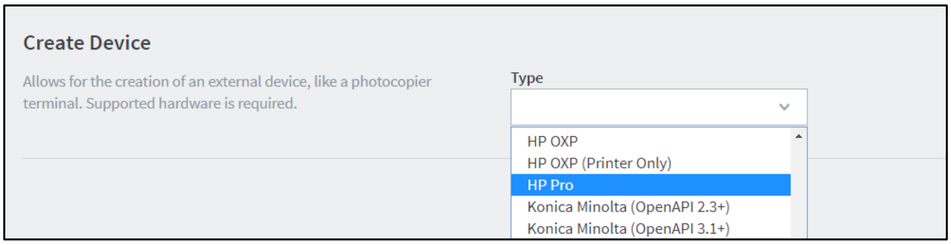
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **External Hardware Integration** area, select **Enable external hardware integration (for supported devices only)**.

   External Hardware Integration

   ☑ Enable external hardware integration (for supported devices only)

4. Click **Apply**.
5. Navigate to **Devices.**
6. Click **Create Device.**
7. In **Type**, select **HP Pro**:

   Create Device

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

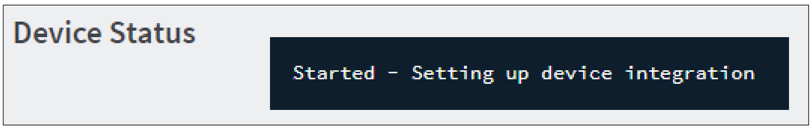
   Type

   HP OXP
   HP OXP (Printer Only)
   HP Pro
   Konica Minolta (OpenAPI 2.3+)
   Konica Minolta (OpenAPI 3.1+)

8. In **Device name**, enter a descriptive name for the device.
9. Optionally, in **Location/Department**, enter location or department details of the device.
10. In **Hostname / IP**, enter the network name or IP address of the device.

    Note: If specifying the device's IP address, ensure this is in the IPv4 format. For more information, see 6.4 Only the IPv4 format of the device's IP address is accepted.
11. In **Device's administrator username** and **Device's administrator password**, enter the same Administrator credentials (username and password) as that of the device's web interface.
12. In **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. For more information on configuring the printer queue's Hold/Release Queue Settings, see the PaperCut MF manual.
13. Click **Ok**.

    PaperCut MF's installation on the device (i.e. device registration and integration) starts:

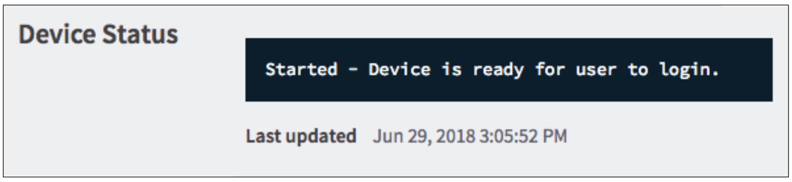
    

    Device Status

    Started - Setting up device integration

14. Verify that PaperCut MF is installed on the device (i.e. device registration and integration is completed):

    The **Device Status** displays the status **Started - Device is ready for user to login**:

    Device Status

    Started - Device is ready for user to login.

    Last updated Jun 29, 2018 3:05:52 PM

Note: If the **Device Status** displays any other status, then see 8.2 Device Status "Started (with errors)" or 8.3 Device Status "Stopped (with errors)"

15. If 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. For more information, see 5.3 "Swipe card" authentication method and 5.3.3 HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader.
16. *PaperCut MF - HP Pro (Fast Release)* currently allows the use of only registered swipe cards that do not require a PIN and that have already been associated with users. As a result, ensure that all swipe cards are registered and associated with users. For more information, see 5.3 "Swipe card" authentication method and 5.3.1 Synchronizing card identifiers and users.

4 Post-install testing

After PaperCut MF is installed on the device (i.e. device registration and integration have been 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.

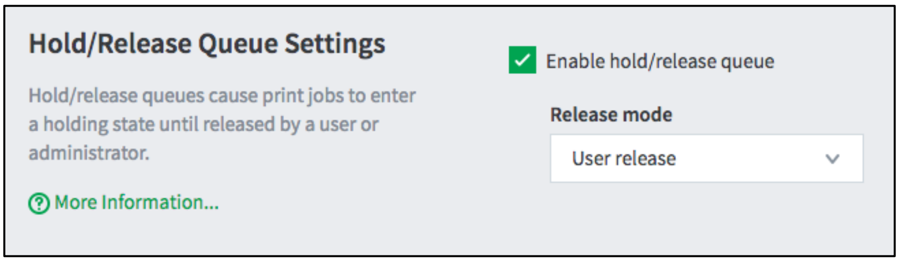
This section covers the following post-install testing scenario for *PaperCut MF - HP Pro (Fast Release)*:

- 4.2 Simple printing

4.1 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**.



Hold/Release Queue Settings

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

More Information...

☑ Enable hold/release queue

Release mode

User release

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

- **Device queue settings** – The device is configured with at least one applicable source queue for print release that corresponds to this device's configured printer queue. For more information, see 3.4.1 Install PaperCut MF.

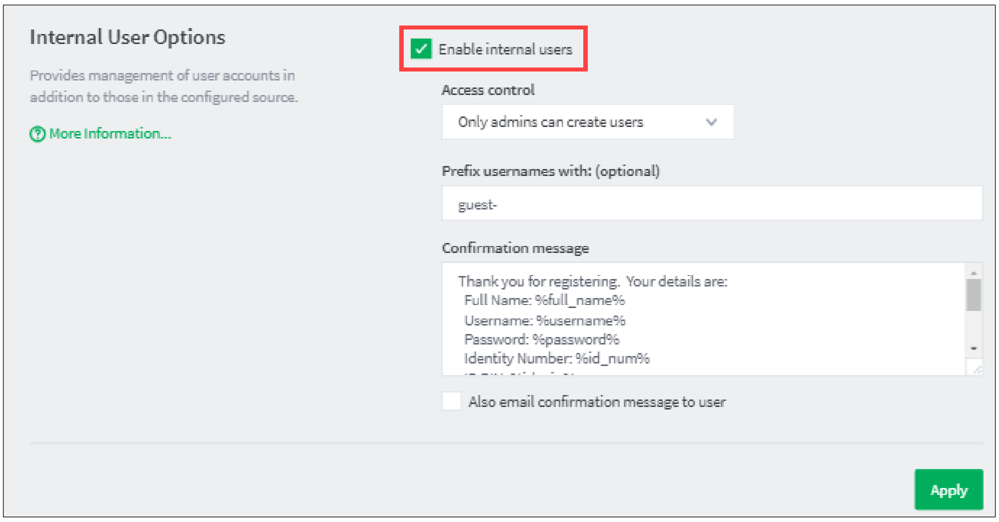
  To configure the device with at least one applicable source queue for print release:

  1. Log in to the PaperCut MF Admin web interface.
  2. Navigate to **Devices**.
  3. Select the device being tested.
  4. In the **Print Release** area's field **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.
  5. Click **Apply**.
  6. 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 using a registered swipe card, is created and configured.

  To create and configure a test user with a registered swipe card:

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



Internal User Options

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

☑ Enable internal users

Access control: Only admins can create users

Prefix usernames with: (optional): guest-

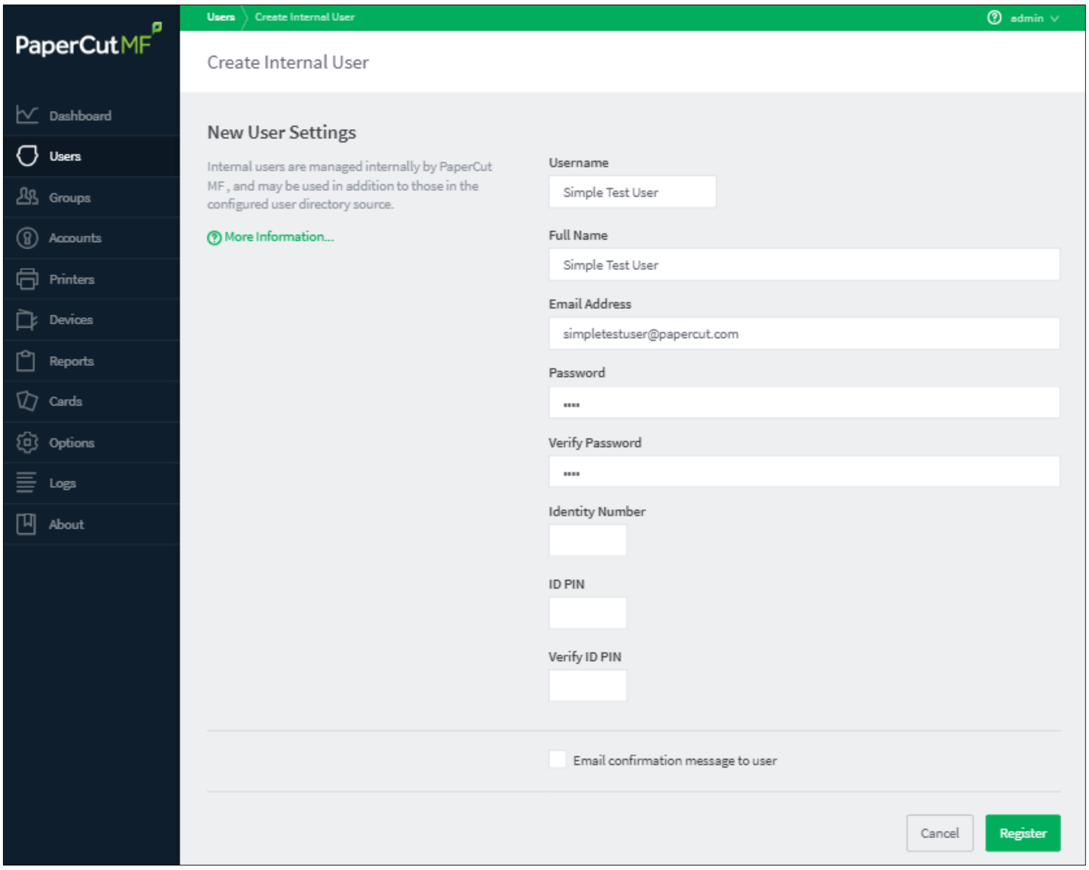
Confirmation message:

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

☐ Also email confirmation message to user

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

7. Enter the relevant details for the test users as required (simple test user):



Create Internal User

New User Settings

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

Username: Simple Test User

Full Name: Simple Test User

Email Address: simpletestuser@papercut.com

Password: ••••

Verify Password: ••••

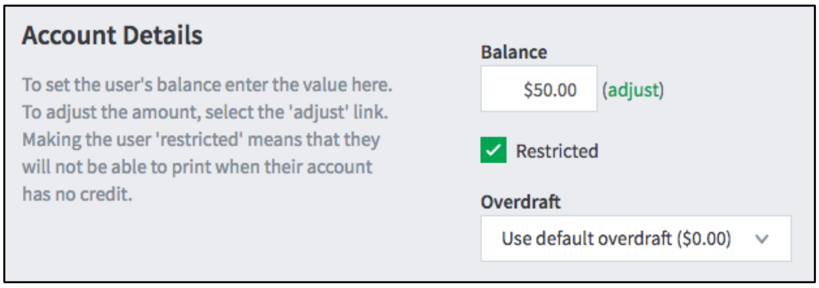
Identity Number:

ID PIN:

Verify ID PIN:

☐ Email confirmation message to user

8. Click **Register**.
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:**



Account Details

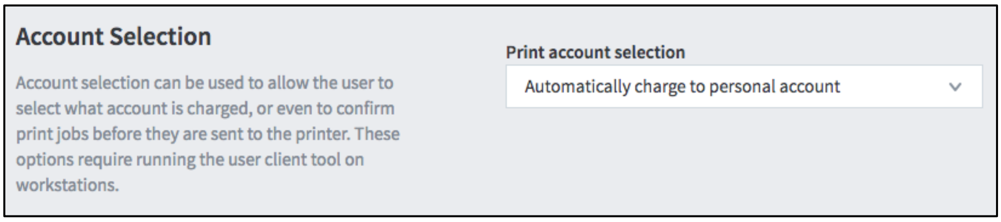
To set the user's balance enter the value here. To adjust the amount, select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance: $50.00

☑ Restricted

Overdraft: Use default overdraft ($0.00)

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

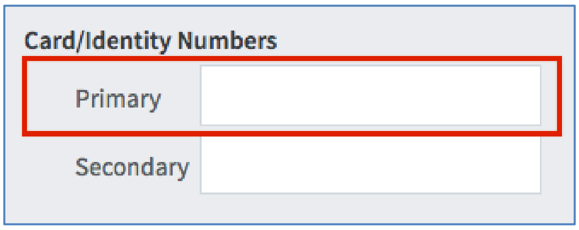


Account Selection

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

Print account selection: Automatically charge to personal account

13. In the **Other Details** area's **Card/Identity Numbers**, enter the card number of the swipe card that is used by the simple test user:



14. Click **Apply**.

4.2 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.

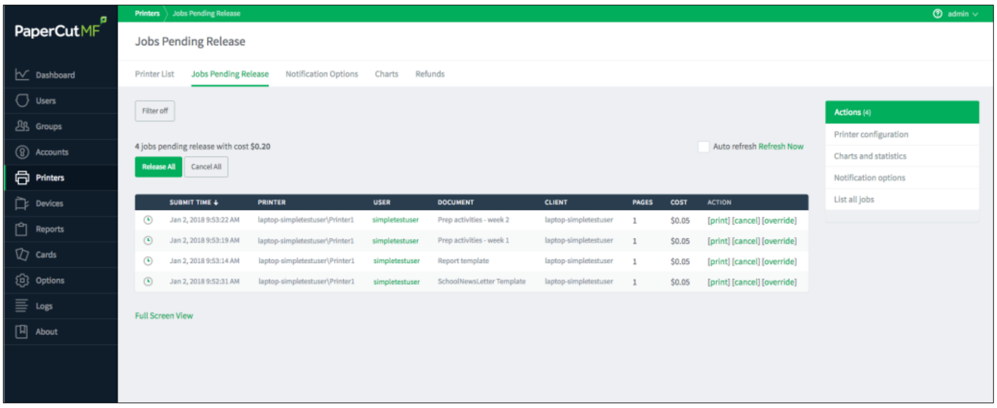
To test simple printing, ensure the following requirements are met:

- **Printer queue settings** – The printer queue's Hold/Release Queue Settings are configured.
- **Device queue settings** – The device is configured with at least one applicable source queue for print release that corresponds to this device's configured printer queue.
- **Simple test user** – A simple test user who performs simple printing is created and configured.

For more information, see 4.1 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:

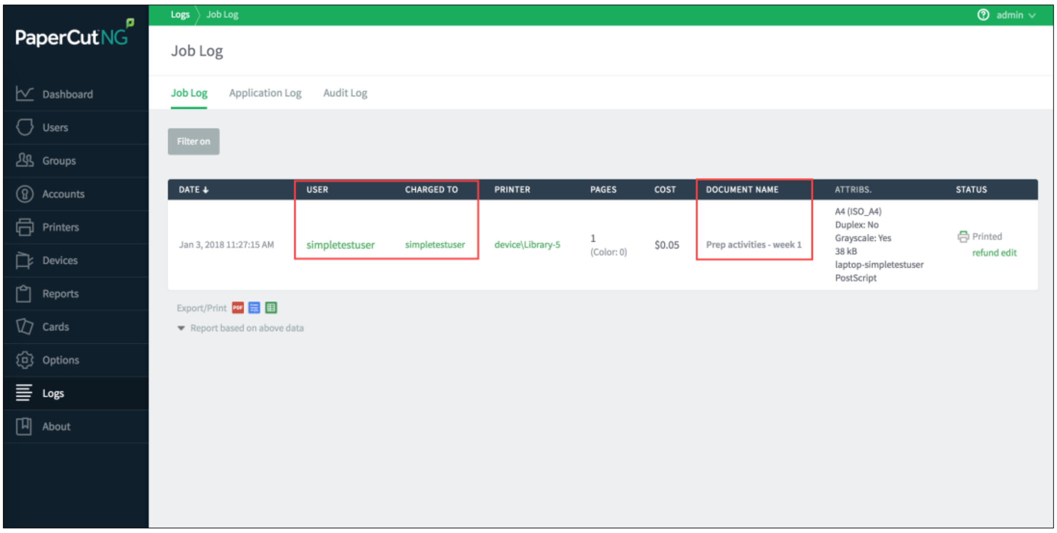


4 jobs pending release with cost $0.20

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

6. Log out of the PaperCut MF Admin web interface.
7. Using the simple test user's registered swipe card, swipe to log in to the device as the simple test user.
8. Verify that all the held print jobs for the simple test user are released and printed on successful authentication.
9. Log out of the device.

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



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

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

5 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 Pro (Fast Release)*.

5.1 Inbound connections

5.1.1 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 5.4 Config Editor.

5.1.2 Inbound connections to PaperCut MF Site Servers

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

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

5.2 Security settings

5.2.1 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.

To enable HTTPS, you must use an RFC5280-compliant **self-signed SSL certificate** or a **CA-signed SSL certificate**:

- **Self-signed SSL certificate –** To use a self-signed SSL certificate from a third-party library (for example, OpenSSL) or 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.
        - that the `<-bcCa>` parameter contains the Basic Constraints CA extension included and the `<SYSTEM-NAME>` parameter contains the PaperCut MF Application Server's IP address either in the **Common Name** (CN) field or in the **Subject Alternative Name** (SAN) field extension of the certificate. 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, and does not include a Basic Constraints CA extension.

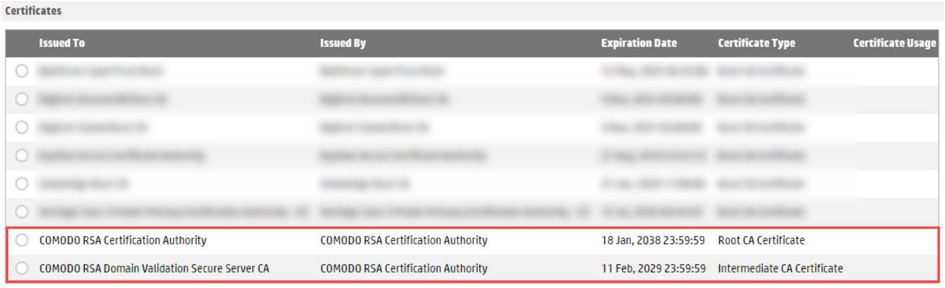
  - that the keystore location always contains only one, most recently generated self-signed certificate.

  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 5.4 Config Editor.
4. It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 5.4 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 PaperCut MF Application Server's IP address in the **Subject Alternative Name** (SAN) field extension of the certificate. This is because CA-signed SSL certificates are issued using a fully qualified domain name (or wildcard), instead of the IP address.
  2. Set the config key **ext-device.hp-oxpd.use-ssl** to **Y**. For more information, see 5.4 Config Editor.
  3. It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 5.4 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:



Certificates

	Issued To	Issued By	Expiration Date	Certificate Type	Certificate Usage
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	[illegible]	[illegible]	[illegible]	[illegible]	
○	COMODO RSA Certification Authority	COMODO RSA Certification Authority	18 Jan, 2038 23:59:59	Root CA Certificate	
○	COMODO RSA Domain Validation Secure Server CA	COMODO RSA Certification Authority	11 Feb, 2029 23:59:59	Intermediate CA Certificate	

     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**.

To test HTTPS:

1. Verify that you are able to log in to the device as a test user (simple test user) and release held print jobs on successful authentication.

5.2.2 Additional network security (optional)

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 on the PaperCut MF Admin web interface:

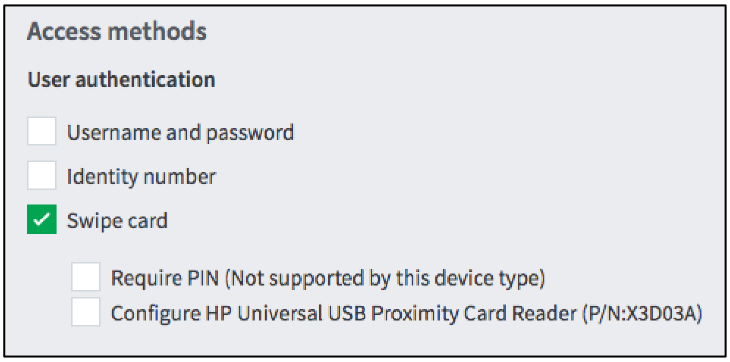
1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Options > Advanced**.
3. In the **Security** area's field **Allowed device IP addresses**, enter a comma-separated list of device IP addresses or subnets (<ip-address1 or subnet-mask1>, <ip-address2 or subnet-mask2>).
4. Click **Apply**.

5.3 "Swipe card" authentication method

PaperCut MF provides you with the **Swipe card** authentication method to authenticate users when logging in to PaperCut MF on the device. Swiping to log in also causes all held print jobs to be automatically released and printed on successful authentication.

To access the **Swipe card** authentication method on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
   The **Swipe card** authentication method is in the **Device Details** page's **External Device Settings** section:



Access methods

User authentication

☐ Username and password
☐ Identity number
☑ Swipe card
  ☐ Require PIN (Not supported by this device type)
  ☐ Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)

Note:

- You can use only the **Swipe card** authentication method (all other authentication methods are unavailable and cannot be used). For more information, see 6.2 Only the "Swipe card" authentication method is available.
- Within the **Swipe card** authentication method, only the **Configure HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader** option is available (all other options are unavailable and cannot be used). For more information, see 6.3 Swiping to log in is available only for registered swipe cards without PIN.

  - If you are using the HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader, then you must it configure it to read the card types being used. For more information, see 5.3.3 HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU Card Reader.

5.3.1 Synchronizing card identifiers and users

PaperCut MF - HP Pro (Fast Release) currently allows the use of only registered swipe cards that do not require a PIN and that have already been associated with users. For more information, see 6.3 Swiping to log in is available only for registered swipe cards without PIN.

As a result, ensure that all swipe cards are registered and associated with users. For more information, see the PaperCut MF manual.

5.3.2 Supported card readers

PaperCut MF - HP Pro (Fast Release) supports the following configured and compatible card readers on HP Pro devices:

- HP Universal USB Proximity Card Reader (Part Number X3D03A)
- RF IDeas RDR-805H3AKU
- RF IDeas RDR-8051AKU
- 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)
- Securakey ET4-AUS-Ds

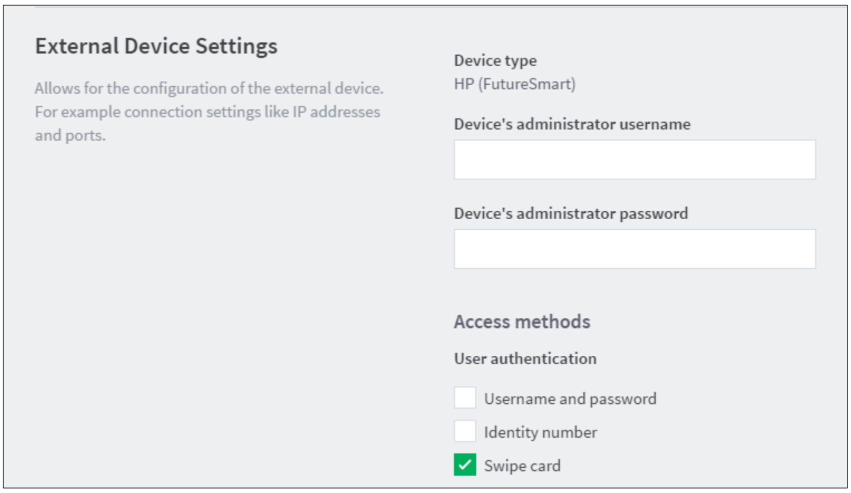
Note: In addition to the above card readers, you may customize *PaperCut MF - HP Pro (Fast Release)* to support other card readers on HP Pro devices by using the config key **ext-device.hp-oxpd.additional-card-readers.vid-pid.hex**. For more information, see 5.4 Config Editor.

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

If 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 on the PaperCut MF Admin web interface:

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



External Device Settings

Allows for the configuration of the external device. For example connection settings like IP addresses and ports.

Device type
HP (FutureSmart)

Device's administrator username

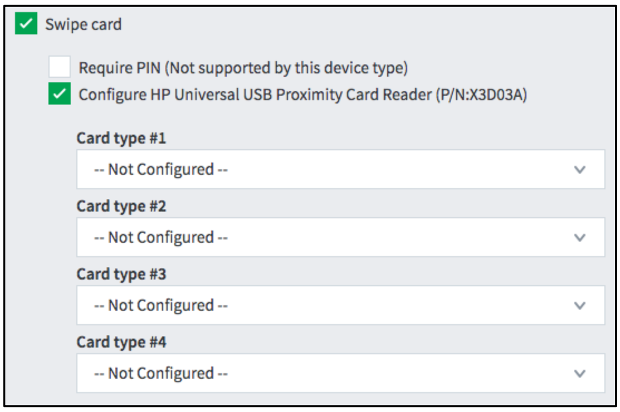
Device's administrator password

Access methods

User authentication

☐ Username and password
☐ Identity number
☑ Swipe card

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



☑ Swipe card

☐ Require PIN (Not supported by this device type)
☑ Configure HP Universal USB Proximity Card Reader (P/N:X3D03A)

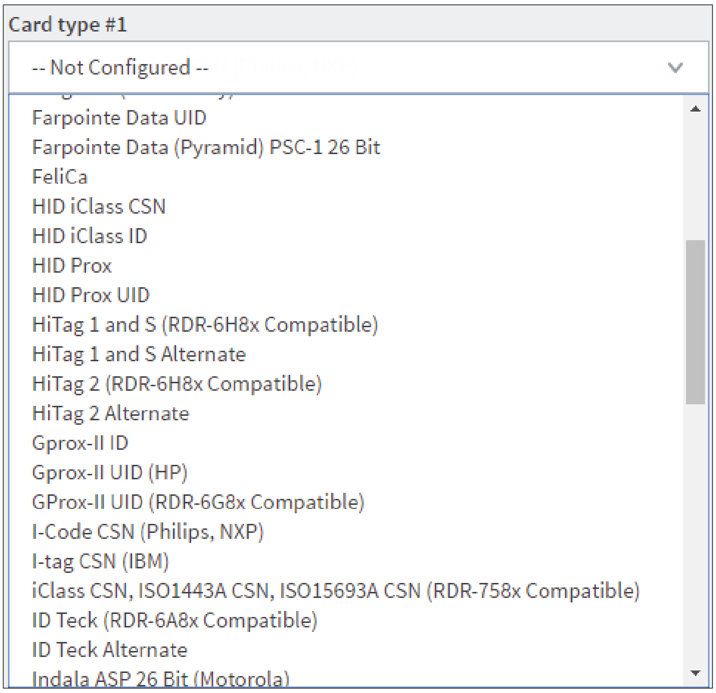
Card type #1
-- Not Configured --

Card type #2
-- Not Configured --

Card type #3
-- Not Configured --

Card type #4
-- Not Configured --

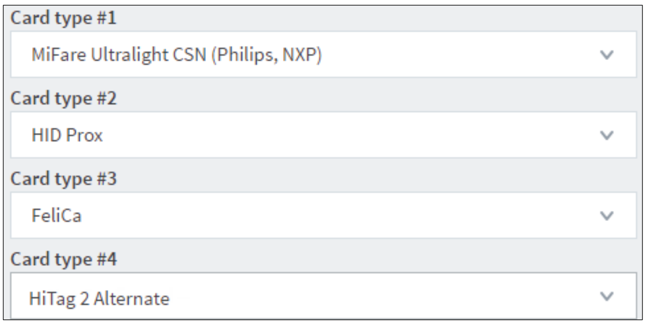
6. Select the card type to be read by your HP Universal USB Proximity Card Reader (Part Number X3D03A) or RF IDeas RDR-805H3AKU card reader:



Card type #1
-- Not Configured --

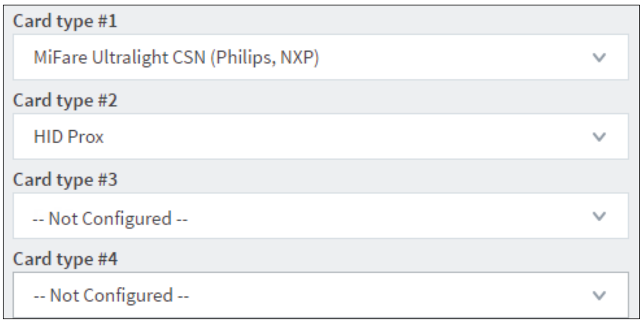
Farpointe Data UID
Farpointe Data (Pyramid) PSC-1 26 Bit
FeliCa
HID iClass CSN
HID iClass ID
HID Prox
HID Prox UID
HiTag 1 and S (RDR-6H8x Compatible)
HiTag 1 and S Alternate
HiTag 2 (RDR-6H8x Compatible)
HiTag 2 Alternate
Gprox-II ID
Gprox-II UID (HP)
GProx-II UID (RDR-6G8x Compatible)
I-Code CSN (Philips, NXP)
I-tag CSN (IBM)
iClass CSN, ISO1443A CSN, ISO15693A CSN (RDR-758x Compatible)
ID Teck (RDR-6A8x Compatible)
ID Teck Alternate
Indala ASP 26 Bit (Motorola)

- You can configure up to four card types:



Card type #1
MiFare Ultralight CSN (Philips, NXP)
Card type #2
HID Prox
Card type #3
FeliCa
Card type #4
HiTag 2 Alternate

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



Card type #1
MiFare Ultralight CSN (Philips, NXP)
Card type #2
HID Prox
Card type #3
-- Not Configured --
Card type #4
-- Not Configured --

- Some card types conflict with other card types. Hence, avoid selecting such conflicting card types, because this causes some problems when logging in. For more information, see 8.4 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

5.3.4 Methods of handling card identifiers

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

- 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 methods:

- 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 methods within the PaperCut MF embedded solution:
  - 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**.

5.3.4.1 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 5.4 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.

5.3.4.2 Standard format converters

To modify card identifiers using standard format converters, use the config key **ext-device.card-no-converter**. For more information, see 5.4 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.	

5.3.4.3 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 5.4 Config Editor.

5.4 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 access the available global config keys (impact PaperCut MF on all devices) on the PaperCut MF Admin web interface:

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 access the available device-specific config keys (impact PaperCut MF on the selected device) on the PaperCut MF Admin web interface:

1. Log in to the PaperCut MF Admin web interface.

2. Navigate to **Devices.**
3. Select the device.
4. Navigate to **Actions > Config editor (advanced).**

The available config keys are:

Config name	Description
"Swipe card" authentication method	
ext-device.hp-oxpd.registered-card-reader.poll.retry	Customize the number of attempts made by the card reader to connect to the device, after a power supply interruption. This is a device-specific config key. • Values: 0-30 • Default: 10 **Note:** Setting this to 0 – is not recommended. This is because, after a power supply interruption the card reader does not attempt to connect to the device. As a result, it is unavailable for user authentication, preventing users from being able to access the device.
ext-device.hp-oxpd.additional-card-readers.vid-pid.hex	Specify the card readers that are supported by PaperCut MF on HP Pro devices, 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:** For more information, see 5.3.2 Supported card readers.
ext-device.card-no-regex	Customize 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:** For more information, see 5.3.4 Methods of handling card identifiers.
ext-device.card-no-converter	Customize 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:** For more information, see 5.3.4 Methods of handling card identifiers.
Network resilience, security	
system.network-address	Specify the network IP address of the PaperCut MF Application Server that the device uses to make inbound connections. This is a global config key. • Values: Network IP address of the PaperCut MF Application Server used by the device for inbound connections. For more information, see 5.1.1 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** accordingly. For more information, see 5.2.1 HTTPS Security (recommended).
ext-device.hp-oxpd.port-num	Customize 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** accordingly. For more information, see 5.2.1 HTTPS Security (recommended).
ext-device.hp-oxpd.period.ping	Customize 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	Customize 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	Customize 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.

Description of available config keys

6 Known Limitations

6.1 Device screens are unavailable

PaperCut MF - HP Pro (Fast Release) currently caters only to HP Pro devices that either do not have device screens or that have small screens. There are no PaperCut MF screens on the device that users can interact with. Hence, apart from swiping to log in (**Swipe card** authentication method), no other user interaction on the device using device screens is available. Swiping to log in also causes all held print jobs to be automatically released and printed on successful authentication. For more information, see 5.3 "Swipe card" authentication method.

6.2 Only the "Swipe card" authentication method is available

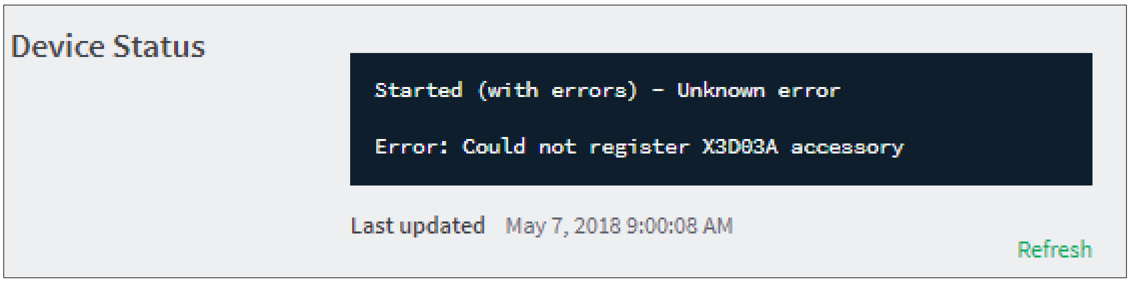
PaperCut MF - HP Pro (Fast Release) currently allows only the **Swipe card** authentication method on HP Pro devices. Users can only use a swipe card when attempting to log in to the device and cannot use any other authentication method. For more information, see 5.3 "Swipe card" authentication method.

6.3 Swiping to log in is available only for registered swipe cards without PINs

PaperCut MF - HP Pro (Fast Release) currently allows the use of only registered swipe cards that do not require a PIN and that have already been associated with users. As a result, ensure that all swipe cards are registered and associated with users. For more information, see 5.3 "Swipe card" authentication method and 5.3.1 Synchronizing card identifiers and users.

6.4 Only the IPv4 format of the device's IP address is accepted

When attempting to create the device (PaperCut MF installation or device registration and integration), if device's IP address is specified in the **Hostname / IP** field, ensure this is only in the IPv4 format. Using IPv6, results in the following **Device Status** error, implying that PaperCut MF installation is unsuccessful:



```
Started (with errors) - Unknown error

Error: Could not register X3D03A accessory
```

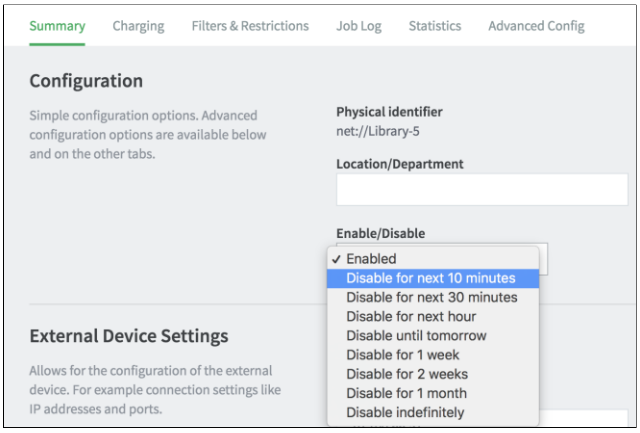
Last updated May 7, 2018 9:00:08 AM

7 Uninstall *PaperCut MF - HP Pro (Fast Release)*

7.1 Temporarily disable *PaperCut MF - HP Pro (Fast Release)*

To temporarily disable *PaperCut MF - HP Pro (Fast Release)*:

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



Configuration

Simple configuration options. Advanced configuration options are available below and on the other tabs.

Physical identifier
net://Library-5

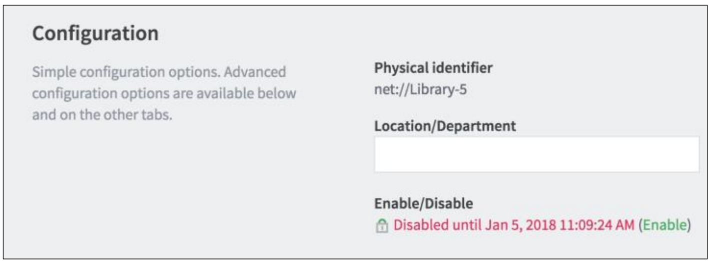
Location/Department

Enable/Disable

External Device Settings

Allows for the configuration of the external device. For example connection settings like IP addresses and ports.

5. Verify that *PaperCut MF - HP Pro (Fast Release)* is disabled:



Configuration

Simple configuration options. Advanced configuration options are available below and on the other tabs.

Physical identifier
net://Library-5

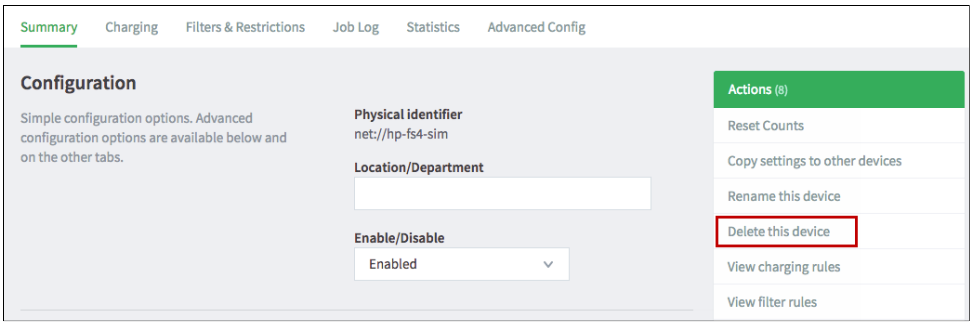
Location/Department

Enable/Disable
Disabled until Jan 5, 2018 11:09:24 AM (Enable)

6. Log out of the PaperCut MF Admin web interface.
5. Using the simple test user's registered swipe card, verify that swipe to log in to the device as the simple test user is unsuccessful and that held print jobs for the simple test user are not released and printed.

7.2 Permanently uninstall *PaperCut MF - HP Pro (Fast Release)*

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



Configuration

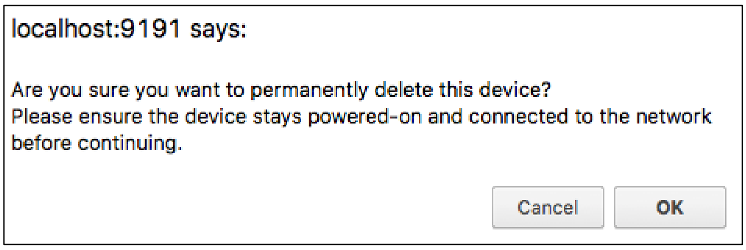
Simple configuration options. Advanced configuration options are available below and on the other tabs.

Physical identifier
net://hp-fs4-sim

Location/Department

Enable/Disable
Enabled

5. Click **Ok:**



localhost:9191 says:

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

6. Click **Devices** and verify that the device is no longer listed (*PaperCut MF - HP Pro (Fast Release)* is permanently uninstalled).
7. Log out of the PaperCut MF Admin web interface.
8. Using the simple test user's registered swipe card, verify that swipe to log in to the device as the simple test user is unsuccessful and that held print jobs for the simple test user are not released and printed.

8 FAQ & Troubleshooting

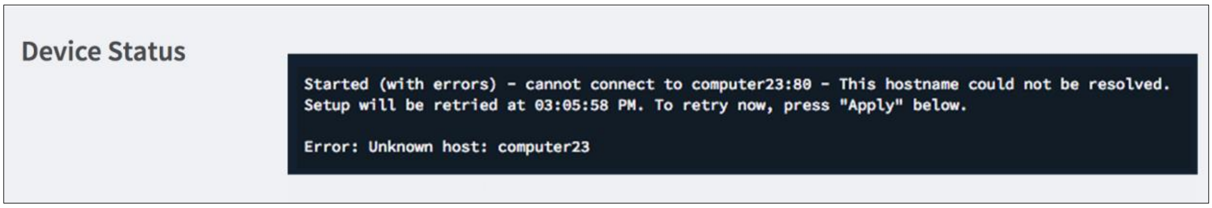
8.1 IP addresses of the PaperCut MF Application Server

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`

8.2 Device Status "Started (with errors)"

After attempting to create the device (PaperCut MF installation or device registration and integration), 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.



Device Status

```
Started (with errors) - cannot connect to computer23:80 - This hostname could not be resolved.
Setup will be retried at 03:05:58 PM. To retry now, press "Apply" below.

Error: Unknown host: computer23
```

To resolve this:

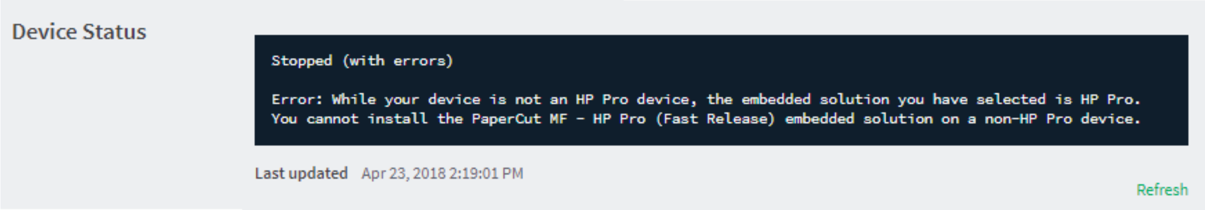
1. Address any device-specific errors outlined on the device.

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**.

8.3 Device Status "Stopped (with errors)"

After attempting to create the device (PaperCut MF installation or device registration and integration), if the **Device Status** displays **Stopped (with errors)**, it implies that PaperCut MF installation is unsuccessful because of any one of the following reasons:

- Either, *PaperCut MF - HP Pro (Fast Release)* is being installed on a non-HP Pro device:

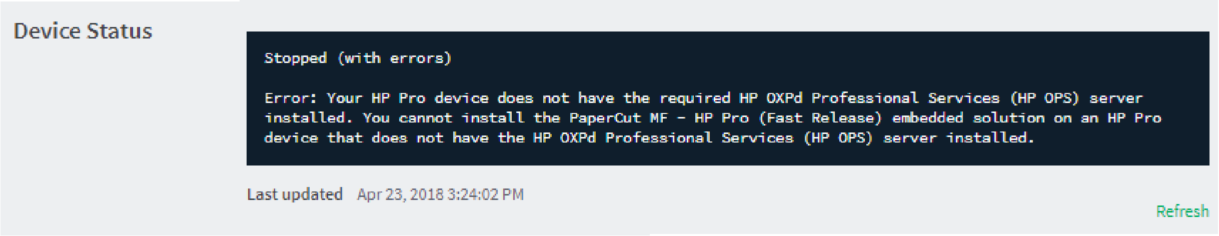


```
Stopped (with errors)

Error: While your device is not an HP Pro device, the embedded solution you have selected is HP Pro.
You cannot install the PaperCut MF - HP Pro (Fast Release) embedded solution on a non-HP Pro device.
```

Last updated Apr 23, 2018 2:19:01 PM

- Or, *PaperCut MF - HP Pro (Fast Release)* is being installed on an HP Pro device that does not have the required HP OXP Professional Services (OPS) server installed:



```
Stopped (with errors)

Error: Your HP Pro device does not have the required HP OXPd Professional Services (HP OPS) server
installed. You cannot install the PaperCut MF - HP Pro (Fast Release) embedded solution on an HP Pro
device that does not have the HP OXPd Professional Services (HP OPS) server installed.
```

Last updated Apr 23, 2018 3:24:02 PM

To resolve this:

1. Log in to the PaperCut MF Admin web interface.
2. Navigate to **Devices**.
3. Select the device.
4. Based on the reason for the error:
   - Either, change the **Hostname / IP** to that of an HP Pro device,
   - Or, ensure that the HP Pro device has the required HP OXP Professional Services (OPS) server installed. For more information, see 9 Appendix A: HP OXP Professional Services (OPS) server.
5. Click **Apply**.

8.4 Swipe card authentication anomalies

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

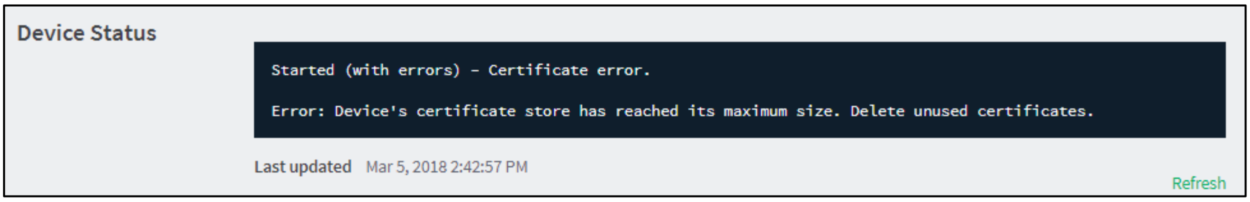
To resolve this:

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

3. Select the 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)

8.5 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:



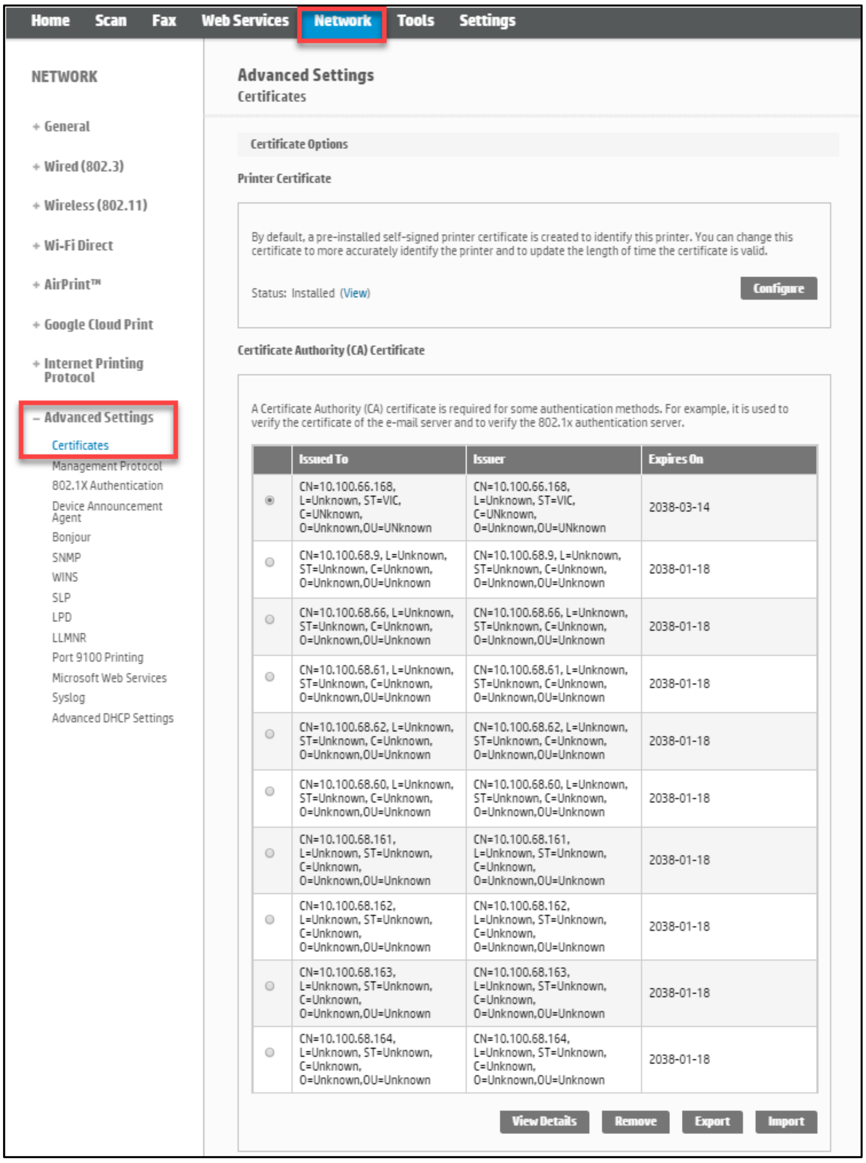
```
Started (with errors) - Certificate error.

Error: Device's certificate store has reached its maximum size. Delete unused certificates.
```

Last updated Mar 5, 2018 2:42:57 PM

To resolve this:

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



Advanced Settings

Certificates

Certificate Options

Printer Certificate

By default, a pre-installed self-signed printer certificate is created to identify this printer. You can change this certificate to more accurately identify the printer and to update the length of time the certificate is valid.

Status: Installed (View)

Certificate Authority (CA) Certificate

A Certificate Authority (CA) certificate is required for some authentication methods. For example, it is used to verify the certificate of the e-mail server and to verify the 802.1x authentication server.

	Issued To	Issuer	Expires On
●	CN=10.100.66.168, L=Unknown, ST=VIC, C=UNknown, O=Unknown,OU=UNknown	CN=10.100.66.168, L=Unknown, ST=VIC, C=UNknown, O=Unknown,OU=UNknown	2038-03-14
○	CN=10.100.68.9, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.9, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.66, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.66, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.61, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.61, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.62, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.62, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.60, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.60, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.161, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.161, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.162, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.162, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.163, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.163, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18
○	CN=10.100.68.164, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	CN=10.100.68.164, L=Unknown, ST=Unknown, C=Unknown, O=Unknown,OU=Unknown	2038-01-18

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

8.6 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:

- 8.6.1 Config keys
- 8.6.2 PaperCut MF Application Server’s IP Address
- 8.6.3 Root and Intermediary Certificates for CA-signed SSL certificates

8.6.1 Config keys

- Ensure the config key **ext-device.hp-oxpd.use-ssl** is set to **Y**. For more information, see 5.4 Config Editor.
- It is recommended that you set the config key **ext-device.hp-oxpd.port-num** to **443**. For more information, see 5.4 Config Editor.

8.6.2 PaperCut MF Application Server's IP Address

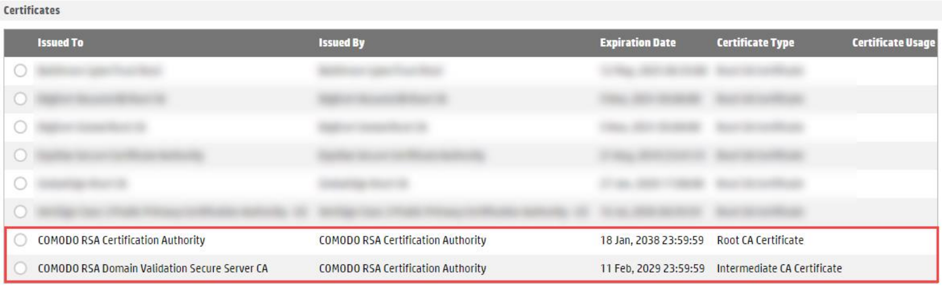
Ensure that the PaperCut MF Application Server's IP address is the same in each of the following:

- 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

8.6.3 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:



Certificates

	Issued To	Issued By	Expiration Date	Certificate Type	Certificate Usage
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	[redacted]	[redacted]	[redacted]	[redacted]	
○	COMODO RSA Certification Authority	COMODO RSA Certification Authority	18 Jan, 2038 23:59:59	Root CA Certificate	
○	COMODO RSA Domain Validation Secure Server CA	COMODO RSA Certification Authority	11 Feb, 2029 23:59:59	Intermediate CA Certificate	

   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**.

9 Appendix A: HP OXP Professional Services (OPS) server

PaperCut MF - HP Pro (Fast Release) can only be installed on HP Pro devices that have the HP OXP Professional Services (OPS) server installed.

Although most HP Pro devices have the OPS server already installed, some other devices may require the OPS server to be manually installed in order to allow *PaperCut MF - HP Pro (Fast Release)* to be successfully installed on such devices.

If *PaperCut MF - HP Pro (Fast Release)* is installed on an HP Pro device that does not have the required HP OXP Professional Services (OPS) server installed, the **Device Status** displays an error, implying that PaperCut MF installation is unsuccessful. For more information, see 8.3 Device Status "Stopped (with errors)".