PaperCut Security Whitepaper

Document Type: **Security Whitepaper** Date of Publication: 02-19-2014

Subject: **PaperCut NG & MF**

Prepared for: **EcoprintQ** PaperCut MF Authorized Solution Center

Summary: This whitepaper describes features available with the implementation of PaperCut NG & MF secure print and copier management, and how the integrity of data and access security is maintained within the PaperCut NG & MF software itself.

Contents

PaperCut Features Security Overview

PaperCut is designed to be a business-critical print management solution that is secure in its implementation and features.

Below are a number of the features that will benefit security-conscious organizations in securing their documents and print/copy management workflow:

Digital signatures and watermarking. PaperCut can apply a watermark to the print job that can contain elements such as print job owner, document name, workstation printed from, as well as a digital cryptographically secure signature. This unique digital signature allows printed pages to be traced back to their origin, discouraging users from being complacent with confidential information.

Print archiving. PaperCut is capable of storing raw and image-based copies of print activity within its environment, giving empowered administrators the ability to review and download printed documents. This powerful feature can be applied with fine-grained permissions, for example retaining student printing while not storing archives of staff printing.

Classification of document security. Leveraging the power of PaperCut's customizable print scripting environment, users can be prompted to classify the security level of a print job, which is recorded for future reference and reporting purposes.

Secure print release. Unlike conventional direct printing, PaperCut can integrate card-swipe user authentication at devices (including two factor authentication), ensuring jobs are only printed when the collecting user is present.

Job anonymization. In some circumstances, even the name and owner of a document can be sensitive. PaperCut supports hiding document names from the visible queues in Windows print queues, as well as preventing the true document name and owner from being logged by the PaperCut application.

Full server-side auditing. All print jobs, system settings and admin login activity is recorded in the PaperCut database ensuring full accountability and auditing of print system activity.

Admin access control levels. Different access control rights can be assigned to users allowing selected system administration tasks (e.g. running reports) to be delegated to non-privileged users without compromising system security.

PaperCut System Security Overview

PaperCut has been developed from day one with security in mind. With its roots in education and the full understanding that college kids “like to hack”, PaperCut’s development processes continually focus on security. At the core of this is the open source-based culture where the majority of PaperCut’s source code is made available to customers. The code has been reviewed by leading education organizations. An example of this was an independent security expert working for a college found an XSRF (Cross-Site Request Forgery) security issue during a review in 2008. This issue was fully disclosed and quickly addressed in subsequent release by the PaperCut development team.

At a software level PaperCut leverages Active Directory (or similar directory-service) security groups for access control. Administrators can be setup with different levels of access. For example, system administrators may have access to all features, while office staff are limited to reports and a sub-set of features such as account management. PaperCut uses SSL/HTTPS for communication and web-based administration ensuring sensitive data like passwords and account information is secured over the network. Internal passwords, if used, are stored in an MD5-hashed format which is seeded by username and salted with a random salt. All security related development is internally assessed and R&D is conducted to ensure we’re meeting best practice.

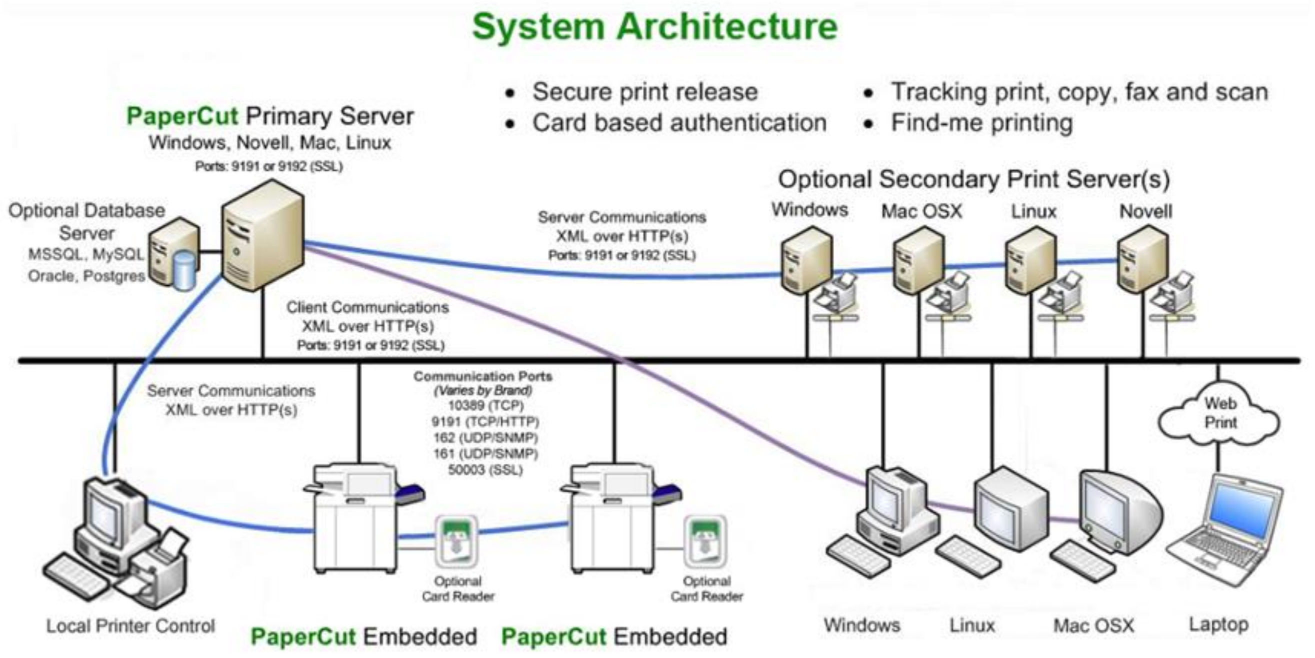
PaperCut also leverages a number of 3rd party components such as the Jetty HTTP Server, Apache Tapestry, Ghost Trap and Apache Derby database. PaperCut actively works with the open source community, backing these projects and has reported and assisted with bugs and issues found over the years. The security of 3rd party components is actively monitored and any security implications, if relevant to PaperCut, are openly addressed. The PaperCut development team has also found security problems in copier/MFP firmware and has worked with leading vendors to address these issues.

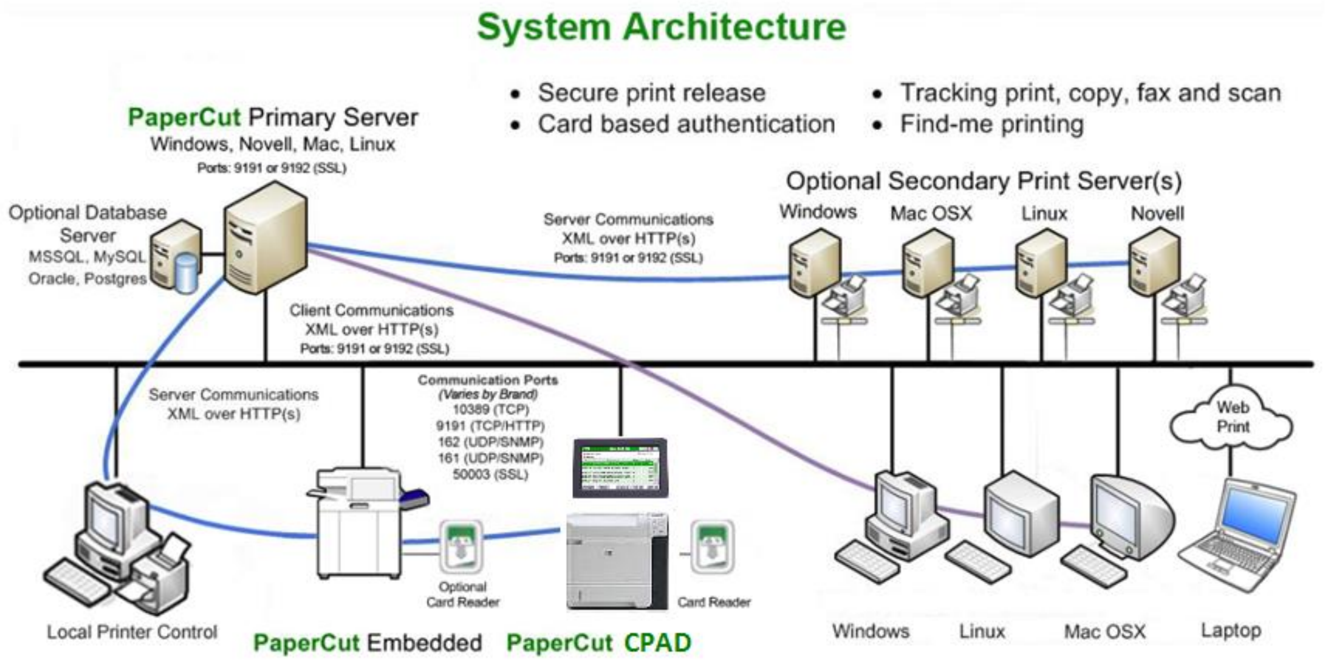
PaperCut is developed in line with security best practices such as CERT Coding Standards, OWASP Top 10, and Oracle Java Security Guidelines. A number of our larger University customers have also had PaperCut subjected to full PCI Security Audits prior to deployment for handling online payments.

The development team regularly review security and add features proactive in line with best-practice (for example, the introduction of HTTPOnly cookie headers added in version 11.2). Another example would be the Ghost Trap project. This is a best practice security related project instigated by PaperCut, aimed to bring best-of-breed security to the Ghostscript Interpreters by sandboxing with the same technology used in the Google Chrome browser.

PaperCut System Security – Network Communication

Communication between different PaperCut modules follows industry best practice, using proven protocols and methods. The following diagram illustrates PaperCut's system architecture with an overview of common communications.





The main network TCP ports used by PaperCut are:

- 9191 for HTTP connections
- 9192 for secure HTTP/SSL connection
- 9193 for device RPC (only used for embedded copier/MFP solutions)

UDP ports are not used for connections from PaperCut client to the sever, only standard TCP. All connections are made inbound from clients and secondary servers to the primary server. No outbound connections are made by the primary server to any workstation or secondary server.

PaperCut uses standard HTTP XML WebServices for client-server and server-server communication (XML-RPC). Sensitive data is sent over SSL/HTTPS on port 9192. The PaperCut installer on Windows and Mac will endeavor to make sure these ports are open. Linux systems running firewalls may need to manual open these ports to local network IP addresses as appropriate.

Client/Server Communication

The configuration of print queues and sending of print jobs between workstations and servers is not affected by PaperCut.

The optional client software communicates with the primary PaperCut server via XML over HTTP on port 9191 for unencrypted traffic and port 9192 for encrypted traffic. Each client maintains a connection using an advanced "long polling" style communication for fast delivery of notifications. Message data is send as required, e.g. when sending a notification or instructing the client tool to display a pop-up. The client software does not accept incoming connections.

The optional client software communicates only with the primary PaperCut server. Communication with external systems is instigated only from the primary server for security and convenience.

Server/Server Communication

Secondary print servers, if configured, communicate via XML over HTTP with the primary PaperCut server on port 9191. Summary print job data is sent to the primary server for logging and analysis, with raw spool data being transmitted based on enabled print archiving options. The primary server replies instructing the secondary server what to do with the print job (e.g. print, cancel, hold pending release). Secondary servers do not accept incoming connections.

Server/External Server Communication

The primary PaperCut server may communicate with an external database for data storage and retrieval. Data is sent and received on demand with intelligent caching taking place within the application server.

The primary PaperCut server may communicate with user directories including Windows Active Directory, Apple Open Directory, Novell eDirectory, and other LDAP servers. User and group information is synchronized automatically overnight, as required, manually or when activated via a script/programming interface. Communication with Active Directory may use the native Windows ADSI APIs or LDAP. LDAP communication uses LDAPv3 and may be encrypted (LDAPS).

The primary PaperCut server may communicate with an SMTP server/service via SMTP, for sending email notifications. STARTTLS can be enabled to encrypt email communications after the initial connection.

The primary PaperCut server retrieves news and upgrade information from www.papercut.com when accessing the “About” section of the administrative interface.

Complete Port Listing

SNMP - for toner level retrieval

- 161 UDP – Outbound. PaperCut connecting to the device.

Cross-Server Job Redirection - the Windows Spooler service uses these port for redirecting print jobs between a Primary and Secondary server.

- 445 TCP – Server Message Block.
- 137/138 UDP – Name and Datagram Services. If using NetBIOS.
- 139 TCP – Session Services. If using NetBIOS.

Google Cloud Print - PaperCut needs to be able to communicate, without the use of a proxy, to the Google Cloud Print services.

- 443 TCP (HTTPS) – with connections to:
  - https://www.googleapis.com/*
  - https://accounts.google.com/*
  - https://www.google.com/cloudprint/*
- 5222 TCP (XMPP, using STARTTLS) – with a persistent connection to:
  - talk.google.com

Device Connections - PaperCut MF uses a variety of port for connecting to copiers, MFPs and other devices. These are listed below by device. Inbound connections are initiated by the device to PaperCut, outbound are initiated by PaperCut to the device.

Cartadis CopiCode-IP

- Inbound
  - 5114
  - 9193

Cartadis cPad

- Inbound
  - 9191
  - 9192

HP

- Inbound
  - 9193

Konica-Minolta

- Outbound
    - 50003
    - 80/443
- Inbound
    - 9191
    - 9192

Kyocera

- Inbound
    - 9191 (if using custom logos)
    - 9193

Lexmark

- Inbound
    - 9191 (if using custom logos)
    - 9193

Ricoh

- Inbound
- 9193

Samsung

- Inbound
- 9191 (if using custom logos)
- 9193

Sharp

- Outbound
    - 80
    - 443
- Inbound
    - 9191
    - 9192

Toshiba

- Inbound
    - 9191 TCP
    - 10389 TCP
    - 162 UDP (SNMP traps) for SDK1 only
- Outbound
    - 161 UDP (SNMP) for SDK1 only
    - 49629 TCP (HTTP) for SDK2 only

VCC Terminals

- Outbound
    - 1234
    - 1235

Xerox

- Outbound
  - 80
  - 443
- Inbound
  - 9191
  - 9192

Forcing use of HTTPS/SSL only

By default, PaperCut offers both plain HTTP and encrypted HTTPS based browser access. HTTP is on port 9191 and HTTPS/SSL on port 9192. To restrict end-user and admin access to the system via SSL only:

1. Login as an admin level user
2. Navigate to **Options -> Advanced -> Security** (Prior to 13.1 this option is location in **Options -> Client Software**)
3. Select **Use HTTPS/SSL if available**
4. Click Apply to save.

If the **Use SSL/HTTPS if available** option is selected, any users that hit the plain HTTP pages will automatically be redirected to the HTTPS secure connection. Logins via the non-SSL connection will be denied.

> **Note:** Prior to 13.1 Administrator logins were not automatically redirected. An administrator could choose if their login used SSL or plain text connections.

Students/End-User Pages

End-users access the system via the URL: http://server:9191/user or via the Details… link on the client. When the **Use SSL/HTTPS if available** option is selected access to end-user web pages will redirect to the SSL login page.

If you are using the PaperCut user client you should configure the client using the “config.properties” file to connect to the server’s fully qualified address (i.e. the name the SSL certificate is issued with). This will avoid the certificate warning when the user clicks on the “Details…” link in the client.

> **Note:** When using SSL with end-users we recommend considering a signed certificate with your server. More details about this are found in the manual - http://www.papercut.com/products/ng/manual/apdx-ssl-key-generation.html.

Admin Pages

The admin pages are accessed via URLs like http://server:9191/admin or https://server:9192/admin for a secure connection. This URL is not published anywhere and you should ensure that:

- You only bookmark and use the secure link when accessing from a remote system.
- Only tell other admin/staff the 9192 HTTPS address and bookmark it for them in their browsers. A handy way to publish the URL is to put a convenient link on an intranet page available to all staff.

In the case SSL fails (like if the certificate becomes invalid), administrators will still able to login. However, their request must originate from the PaperCut server's localhost address (127.0.0.1 or 0:0:0:0:0:0:0:1). This is usually done by logging into the PaperCut server (either physically or via a remote desktop connection) and using a browser installed locally.

It is not possible to turn off the plain HTTP port entirely because:

- It is used internally by the client for non-sensitive data such as event notification, as plain HTTP connections have less overhead than SSL, reducing load on the server.
- Will still be available for login.

[The remainder of this page has been intentionally left blank.]

PaperCut Browser Security

PaperCut implements numerous best practises with regards to browser security. Each of these options is enabled by default, balancing where possible practicality and user feedback with an effort to minimize vulnerabilities in a standard configuration.

Web Session Inactivity Timeout

For security reasons all the web sessions log out (timeout) after periods of inactivity. Clicking a link or refreshing a page will reset the inactivity timer. Closing the browser window/tab will also end the session (i.e. the session cookies are not persistent). The default timeout periods for different login types are described in the table below:

Login Type	Default Value
Admin web interface	1440 minutes / 24 hours
Web-based release station	1440 minutes / 24 hours
Web Cashier	1440 minutes / 24 hours
User web interface	60 minutes / 1 hour

These timeout values (a period given in minutes) are configurable via the config keys below. A value of 0 indicates that the session will never time out. The special value DEFAULT indicates that the PaperCut defaults (in the above table) are used. Please note that the PaperCut defaults may change in future versions.

Configuration key name	Description
web-login.admin.session-timeout-mins	Inactivity timeout for the admin web interface
web-login.release.session-timeout-mins	Inactivity timeout for the web-based release station
web-login.web-cashier.session-timeout-mins	Inactivity timeout for Web Cashier
web-login.user.session-timeout-mins	Inactivity timeout for the user web interface

Please see the relevant manual chapter - http://www.papercut.com/products/ng/manual/sys-mgmt-config-editor.html - for information about changing config keys.

Changing the inactivity timeout values will take effect the next time users log in. Note that some pages periodically refresh the page (or data on the page), such as the dashboard and the web based release station. Sessions will not time out if a browser is left on these pages, as they will be considered active.

Web Login Credentials Save and Autocomplete

For security reasons, PaperCut by default disables the login credentials caching and autocompletion browser behaviour. If there is a need for this to be allowed for users, the following key can be set.

Configuration key name	Description
auth.web-login.autocomplete	Specify Y to enable browser auto-completion of the login fields as a convenience to users. By default, the browser is requested to not use auto-completion.

Please see the relevant manual chapter - http://www.papercut.com/products/ng/manual/sys-mgmt-config-editor.html - for information about changing config keys.

PaperCut System Security – Common Questions

Does PaperCut store any passwords?

User authentication is performed by the operating system - usually via a directory service such as Active Directory or LDAP. PaperCut does not store any user passwords and instead interrogates the directory service in real-time. Caching or storing passwords is regarded as a security risk. The only exceptions to this rule are the built-in admin user account and PaperCut internal accounts.

The built-in admin password is stored in a one-way salted hashed format in the server.properties file. This account is kept separate from the directory user accounts ensuring that administrator level login is still possible even during a directory outage.

Internal user passwords are stored in the PaperCut database as a one-way hash in line with security best practice - an MD5 sum factored from a combination of username + password + a salt. This use of a secure one-way hash ensures that users' passwords are kept private even if someone has access to the PaperCut database.

What level of encryption does PaperCut use?

Client-server communication of sensitive data is conducted over an SSL link - this is an equivalent level of encryption to that used by a web browser connected on an https:// website.

A security analysis tool (e.g. a PCI Compliance Scan) is reporting that PaperCut is configured to accept weak ciphers. How can I address this?

This topic is addressed in detail in the knowledge base article: *SSL Cipher Configuration - removing weak ciphers.* http://www.papercut.com/kb/Main/SSLCipherConfiguration

I am going to use Popup Authentication. What should I consider?

Popup-authentication is an auxiliary authentication method and in general should not be used in preference to a protocol-level authentication system. Popup authentication (IP session based authentication) and its security considerations are discussed in detail in a further section of this whitepaper.

Does PaperCut use HtmlOnly secured cookies?

Yes. As of version 11.2 all session ID information stored in copies are marked as HtmlOnly to help mitigate the risk associated with some XSS attacks.

Can I open port 9191/9192 to the world?

Best practice suggests not exposing any services to the Internet unless required. Having said that, we have designed PaperCut to be secure and with the intention of our users opening the HTTPS port 9192 to the Internet to facilitate services such as:

- Remote administration
- Allowing end-users to login from home to check balances and add credit/quota to their accounts

We have a number of large University/College sites that have opened up PaperCut's port to the Internet since 2005. It is recommended to open port 9192 (the SSL port) rather than the plain text port 9191.

Is PaperCut and associated executable given minimum permission needed for operation? Is the concept of least privilege upheld?

Yes. On Windows, Mac, Novell and Linux PaperCut has been designed to run under non-privileged accounts. Key security processes on Linux that need to be run with elevated privileges such as those used for user authentication are run "out of process" so this higher privileges rights are isolated at the process level. On Windows, PaperCut runs its main process as the SYSTEM account with local access only (no network resource access).

How can I restrict access to the XML Web Service APIs?

Two levels of access control are provided for the web services APIs. The first is that any call needs to pass a valid authentication token (usually the built-in admin user's password). All calls not passing this will be rejected. The 2nd level of security is IP address level filtering. By default PaperCut will only allow calls from localhost (127.0.0.1), and optionally this can be extended to other servers by manually granting that server's IP address. Valid IP addresses/ranges are defined under the Options section.

I've run a security scanner across PaperCut and it's raised a warning. What does this mean?

PaperCut is in use in tens-of-thousands of organizations and many of them use various security analysis and scanning tools. If the issue raised is marked as "high", please raise these with our support team. Many of these systems raise issues not pertinent to PaperCut as a print management application; however we like to assess all on a case-by-case basis and will let you know if our developers think they require action.

Are administrator activities audited?

Yes, as a general rule most major operations such as editing printer details, creating/deleting/modifying user accounts are audited. These audit records appear in the App. Log with a date, details and the user who performed the operation. However, a full level system administrator with read/write file access could in theory edit data files directory to modify the audit trail. Standard PaperCut administrators who have their rights limited to only access the server via the web interface cannot modify these records.

Is PaperCut certified under security standard XYZ?

Formal security certification is a new and emerging industry. PaperCut is already developed in line with leading security guidelines and practices (as covered in other sections of this whitepaper). As applicable formal standards emerge and if there is user demand, we will consider formal certification. At the current time, we don't have any concrete intentions. Issues such as our release-often policy and the fact that many certification standards focus on the installed setup rather than the product itself make certification difficult (e.g. PCI DSS).

Is PaperCut PCI Certified?

PaperCut itself does not handle any credit card transactions directly and hence PCI certification is not required/not appropriate for PaperCut itself. PaperCut interfaces with 3rd party payment gateways to handle credit card transactions (e.g. PayPal, CyberSource, Authorize.Net, etc.) and all credit card gateways/providers supported by PaperCut are PCI DSS certified. When a user makes a payment they are directed through to the providers "hosted pay page" and credit card details are entered on their website directly. PCI certification is not something PaperCut can validate as an application, as certification is implementation and site specific. A number of PaperCut customers (such as Universities) are subject to PCI requirements and the PaperCut servers running on these sites are scanned at least once a month.

Is PaperCut susceptible to SQL Injection attacks?

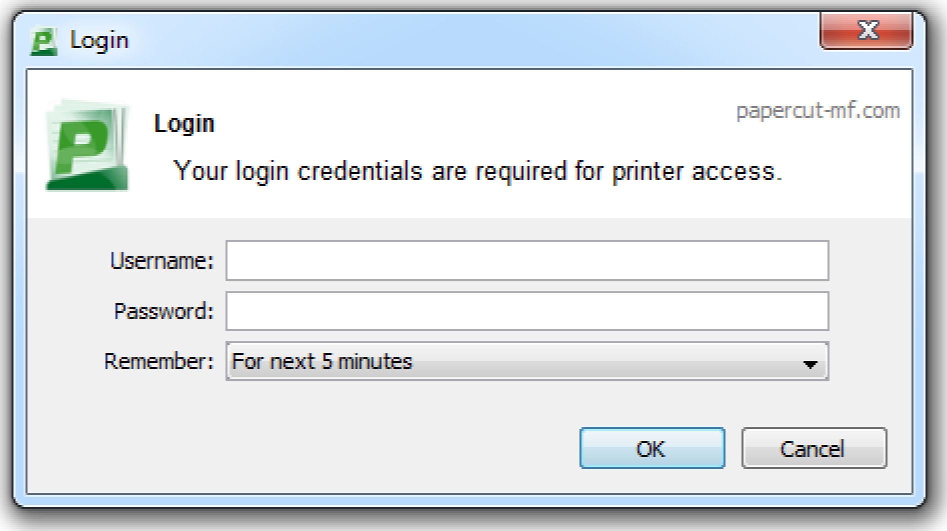
Our coding standard and design policies are designed to limit this type of attack. All database queries in PaperCut are developed using parametrized SQL. This means that PaperCut never directly builds the SQL statement using data provided by the user (e.g. search terms entered in fields). All SQL parameters are handled by the underlying database library which means that PaperCut is not susceptible to SQL injection attacks.

What about the security of any 3rd party libraries and components used by PaperCut?

PaperCut makes use of a number of third party libraries and components. The security of components is actively monitored by our development team and if any are raised, we assess the impact this may have. We take the topic of security for any 3rd component as serious as we do for our own code base. In some situations we have worked with the 3rd party vendors to address security issues. Another example of active 3rd party security management is the Ghost Trap project. This initiative was started by PaperCut and aims to bring best of breed security to the Ghostscript PDL interpreters.

Considerations When Using Popup Authentication

This article relates to Popup Authentication as outlined in the manual - http://www.papercut.com/products/ng/manual/ch-printer-mgmt-popup-auth.html.



Login

Your login credentials are required for printer access.

Username:

Password:

Remember: For next 5 minutes

What is Popup Authentication?

Popup Authentication is a feature in PaperCut which may be used when Protocol-Level Authentication is not available for user print jobs. Typically Popup Authentication is not used as the primary authentication mechanism but is used to support secondary printing services such as desktops that logon under a generic username (i.e. general access PCs in a library) or Mac systems where setting up an authenticated protocol may be beyond available system administration resources. Popup Authentication uses IP-address matching, which is explained in more detail below.

What is Protocol-Level Authentication?

The standard Windows print system is an example of printing using Protocol-Level Authentication. Before a user is able to print, they must be authenticated into the environment (generally a Active Directory domain). Any jobs submitted to the print queue are encapsulated within this authentication as part of the transmission protocol. Due to this, the username with the print event can be trusted for the purposes of accounting and security.

How does Popup Authentication work?

Popup Authentication matches the source IP address of the print job with the user confirmed to be operating from the popup client IP address. The workflow is as follows:

1. The user initiates a print job to a server-hosted, PaperCut-managed, queue (printer) via unauthenticated print protocol.
2. The print job arrives in the print queue and because of the unauthenticated protocol, the username cannot be trusted.
3. PaperCut uses the job's source IP address to determine the PaperCut popup client it should contact for authentication.

4. The user is prompted to enter their credentials, which are then verified against PaperCut's configured directory source. If the credentials are correct, the user is considered authenticated at that client.
5. The print job is attributed to the authenticated user.
6. Depending on configuration, the server may remember the association between the IP address and the authenticated user for a period of time.

When should Popup Authentication be used?

As a general rule, Popup Authentication should only be used in low-volume, low-complexity scenarios when Protocol-Level Authentication has been ruled out. By its design, Protocol-Level Authentication is always the most secure and hence this is the reason why it is used in Windows and authenticated protocols such as HTTP, SSH or Novell's iPrint protocol.

A good example of a situation where Protocol-Level Authentication is not ideal would be a public-access PC in a library set to auto-logon as the insecure, generic account "public". In this case the Protocol-Level Authentication is passing through the insecure user of "public". PaperCut's client software and IP address authentication can overlay these insecure user credentials and request authentication from the user at the time of print via a popup.

What do I need to know when implementing Popup Authentication?

The following is a general guide to factors your System, Network and Security team should consider when implementing Popup Authentication:

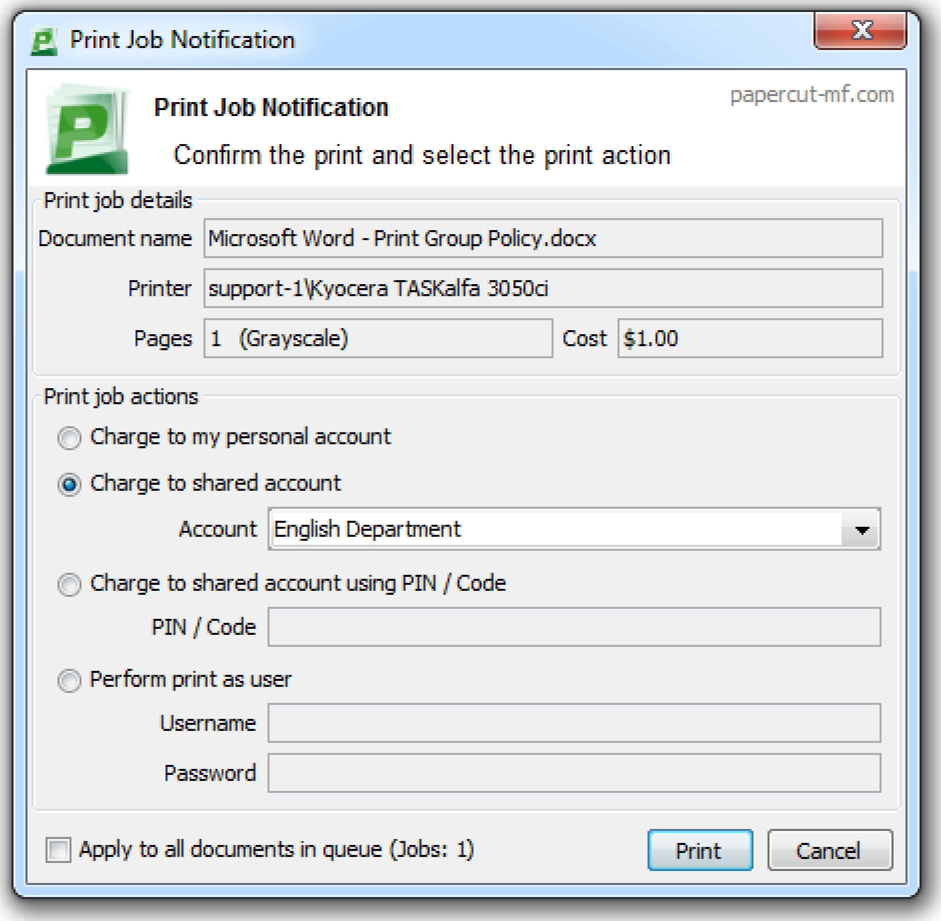
- IP address changes should be minimized. If you are using DHCP, consider the lease time as well as the re-use rate of IP address and DNS scavenging timeouts.
- Do not use any form of NAT between the clients and print server. NAT will obscure the IP address seen by the server.
- Consider the authentication session time (TTL - Time To Live) options offered to your users. This is detailed further in the manual - http://www.papercut.com/products/ng/manual/ch-printer-mgmt-popup-auth.html#table-user-client-popup-auth-config-keys. TTL settings are a trade-off; the shorter the time, the smaller the window of mismatch, but the greater the inconvenience to the user. There is no one-size-fits-all answer; this must be taken on a site-by-site basis.
- Ensure that hostnames can be resolved to IP addresses, both from the client and server. In some situations, hostnames may be reported instead of IP addresses, and resolution results are key to correct behaviour.
- Any machine relying on Popup Authentication must have the PaperCut client running at all times for printing from that workstation to function.
- Awareness of IP address spoofing. Large sites will often actively monitor this and/or endeavour to prevent it, as IP address spoofing is something that affects network application security in general.
- Always reconsider your choice of Popup Authentication. Protocol-Level Authentication may become viable with changes in technology, infrastructure or internal procedure.
- Popup Authentication is not a viable solution for simultaneous multi-user systems such as Terminal Server or Citrix, as multiple users will be reported from a single IP address.

Can you give me a real-life an example of the practical difficulties associated with Popup Authentication?

In 2012 one major university user of PaperCut in the USA was using Popup Authentication to support authentication on print jobs issued via the LPR protocol (for Unix desktop systems). This setup had been in place successfully for 5 years with no reported problems. The site's networking team (independent of the server team responsible for PaperCut's management) decided to make a few network infrastructure changes and enabled NAT for some subnets. The use of NAT caused a subtle set of authentication issues that took a number of days to detect and diagnose. During this time some jobs were incorrectly attributed.

Client Billing Security

By default all printing is automatically charged to the user's personal account. For a user to be able to select a shared account the user needs to be granted access to the account selection popup.



Print Job Notification

papercut-mf.com

Print Job Notification

Confirm the print and select the print action

Print job details

Document name: Microsoft Word - Print Group Policy.docx

Printer: support-1\Kyocera TASKalfa 3050ci

Pages: 1 (Grayscale) Cost: $1.00

Print job actions

○ Charge to my personal account

● Charge to shared account

Account: English Department

○ Charge to shared account using PIN / Code

PIN / Code:

○ Perform print as user

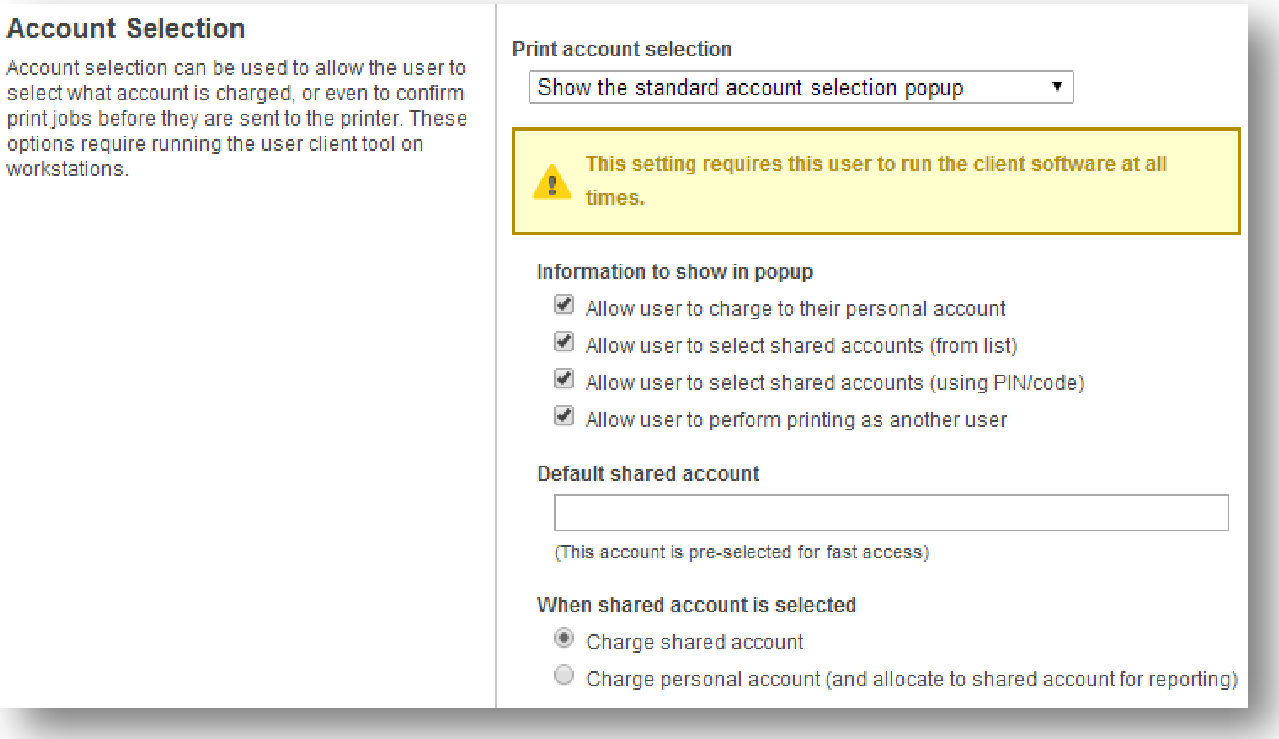
Username:

Password:

□ Apply to all documents in queue (Jobs: 1)

Figure 1. Selecting a shared account from the popup

Access to the account selection popup, as shown in the above figure, is controlled at the user level on the user's details page. The Show the account selection popup option needs to be selected for each user that requires access to shared accounts. System administrators might find the Bulk user actions section under the User List screen convenient for applying this change to many users.



Account Selection

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

Print account selection

Show the standard account selection popup ▾

⚠ This setting requires this user to run the client software at all times.

Information to show in popup

☑ Allow user to charge to their personal account

☑ Allow user to select shared accounts (from list)

☑ Allow user to select shared accounts (using PIN/code)

☑ Allow user to perform printing as another user

Default shared account

(This account is pre-selected for fast access)

When shared account is selected

● Charge shared account

○ Charge personal account (and allocate to shared account for reporting)

Figure 2. The user's popup settings under User -> User Details

> **Note:** It is also possible to automatically charge printing to a single shared account without the need for the popup. This can be useful in environments where a user only ever needs to charge to a single shared account, and it is not desirable to display the popup.

> **Important:** Users need to restart their workstation (or manually restart the PaperCut client software) for this change to take effect. Users with the Show the account selection popup option enabled need to be running the client software at all times. Print jobs will not print until the user has selected the account.

In addition to granting users access to the popup they also need to be granted access to a shared account. Shared accounts access can be controlled using two methods:

- Network group membership
- PINs (also known as security codes or passwords)

If an account is allocated a PIN (an alpha-numeric access code) users with knowledge of the PIN can select the account. A PIN based system would be a sensible selection in an organization when PINs are already in use for other systems such as photocopiers or door access codes.

> **Tip:** PINs/codes can also be used when using parent and sub-accounts. To select a specific sub-account from the client software, both the parent and sub-account pins are required. They should be entered in the format of: [parentPIN]-[subPIN] (i.e. they are separated by a hypen).

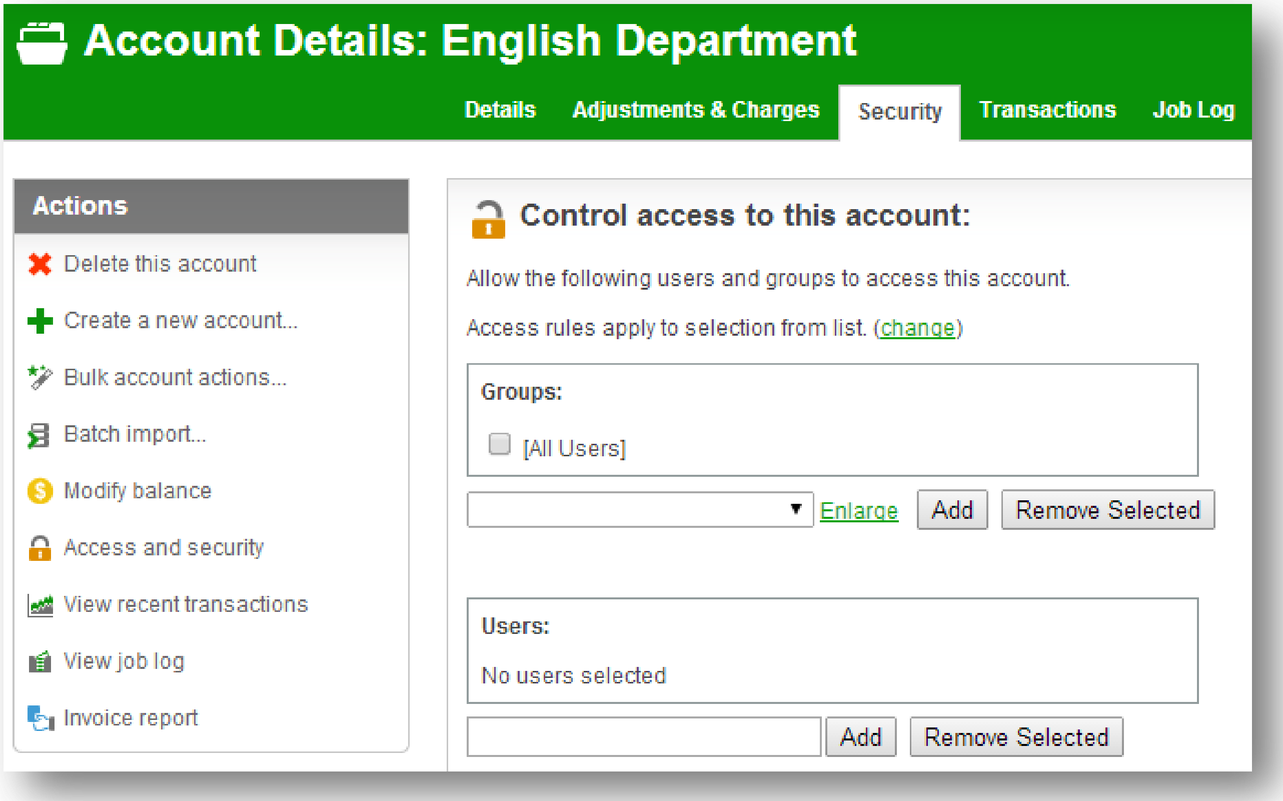
An alternate method is to delegate access to the shared account via network group membership. One advantage of group based control is that users do not have to remember PINs. Most medium to large organizations will already have their network structured into suitable groups representing their position, title, department or work area. These existing groups may be used to control access. Access to shared accounts can also be granted on an individual user basis, however best practice suggests group-based management for medium to large networks.

Tip: In a Windows Active Directory environment, Organization Units are treated as special groups. Hence they also can be used to control access to a shared account.

Controlling access to shared accounts via group membership rather than individual user accounts is recommended. By using group based control, new users created on the network inherit the correct account access by virtue of their network group membership. This alleviates the need for additional user modification inside PaperCut NG.

To grant access to a shared account for all members in a given network group:

1. Log into the system as an administrator (i.e. admin account).
2. Select the Accounts tab.
3. Select the appropriate shared account from the list.
4. Click on the Security tab.
5. Select the appropriate group from the drop-down list.
6. Click the Add button.



Control access to this account:

Allow the following users and groups to access this account.

Access rules apply to selection from list. (change)

Groups:

□ [All Users]

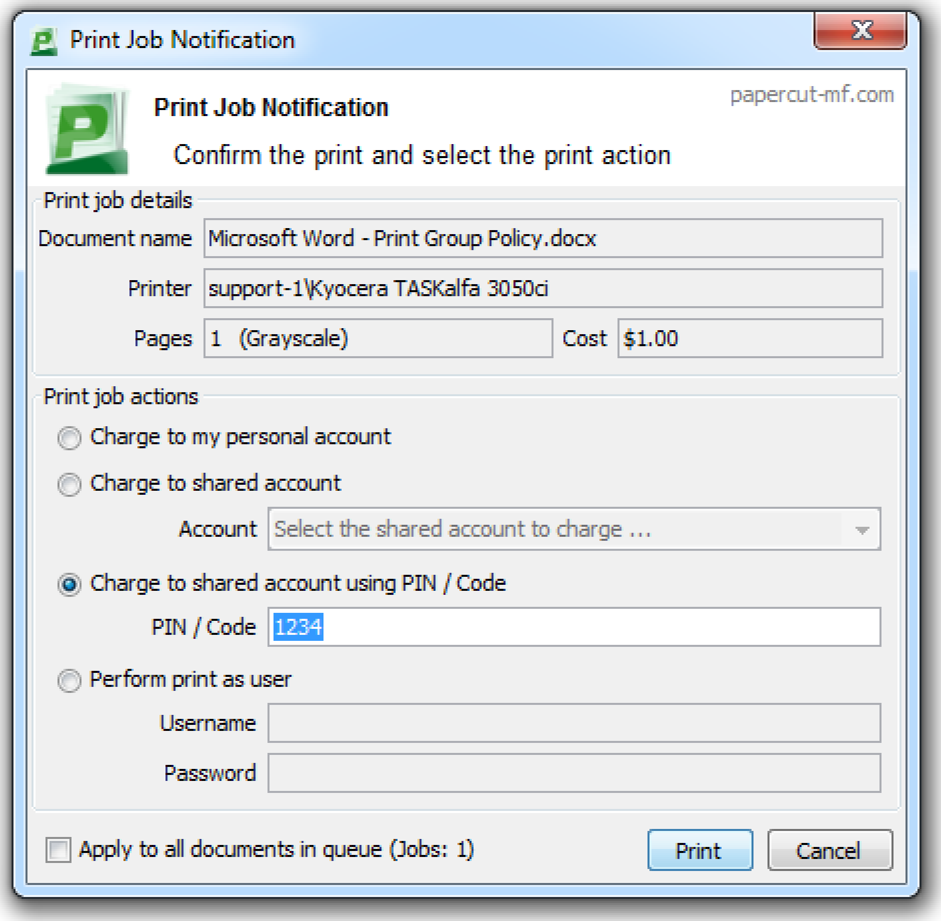
Users:

No users selected

Figure 3. Setting up shared account security

Tip: Security settings of multiple shared accounts can be changed simultaneously by clicking on the Bulk account actions... link under the Accounts tab. More information is available in the section called “Bulk User Operations”.

Using PIN code account security


Print Job Notification

Print Job Notification

Confirm the print and select the print action

papercut-mf.com

Print job details

Document name: Microsoft Word - Print Group Policy.docx

Printer: support-1\Kyocera TASKalfa 3050ci

Pages: 1 (Grayscale) Cost: $1.00

Print job actions

○ Charge to my personal account

○ Charge to shared account

Account: Select the shared account to charge ...

● Charge to shared account using PIN / Code

PIN / Code: 1234

○ Perform print as user

Username:

Password:

□ Apply to all documents in queue (Jobs: 1)

PIN/codes provide a convenient way to select shared accounts. However this convenience may compromise security when short or guessable PINs are used. For this reason PaperCut NG allows the user/group security to be also applied to PIN/code access. This allows sites to use convenient and short codes with confidence that only authorized users are granted access.

To enforce user/group security for PIN/code access:

1. Log into the system as an administrator (i.e. admin account).
2. Go to the Options tab, to the Account Options section.
3. Change the Access rules defined on shared account security tab apply to: setting to both PIN/code and selection from list.
4. Click the Apply button.

With this setting changed, users can only select an account using PIN/code when they:

- know the PIN/code; and
- are in the shared account's user/group security

References and Further Resources

Information contained within this document was sourced from documentation including those listed below. Please refer to these links or your support contact for further clarification:

- http://www.papercut.com/kb/Main/Security
- http://www.papercut.com/kb/Main/CommonSecurityQuestions
- http://www.papercut.com/kb/Main/SSLCipherConfiguration
- http://www.papercut.com/kb/Main/PopupAuthenticationConsiderations
- http://www.papercut.com/kb/Main/ForcingSSL
- http://www.papercut.com/products/ng/manual/ch-shared-accounts-security.html
- http://www.papercut-mf.com/release-history/