A PARTNER GUIDE TO CLOUD SECURITY

Your security is prioritized with PaperCut's built-for-cloud solutions

Are you responsible for locking down data in your organization, or just curious about how PaperCut maintains privacy in the cloud? Let's take a deep dive into the security of our built-for-cloud printing solutions.

Who owns my data?

You do, of course! As outlined in the PaperCut Privacy Policy, all data that goes into our system is your data and we always treat it as such. You can also check out our Privacy & GDPR FAQ.

Who can access my data?

You control who accesses your data by granting and approving administrative rights within your organization. You also have the option to invite third parties – such as your IT service provider or an approved PaperCut partner or reseller – to view your data.

Any time you want to turn on or off access, you have full control to do so.

Like most major online services, PaperCut staff may need to access system data (on rare occasions), such as:

- when legally required to do so, or
- when necessary to ensure that systems and features are working as designed (for example, debugging performance issues, or investigating a reported issue).

By default, this access does not include access to the data in the print document itself, as the data typically remains on-premises, outside of PaperCut's view. If the Cloud Node is enabled, jobs are deleted when they are printed or stored in the cloud for up to 72 hours before being deleted. Access to those documents is controlled by PaperCut's Security Policies.

If access is required, it is limited to a small number of people and controlled by our Data Access Policy, which prohibits access to PaperCut Pocket and PaperCut Hive data except in the above circumstances.

Is my data encrypted?

Data stored and transmitted by PaperCut Pocket and PaperCut Hive is encrypted both in transit and at rest:

- Data stored in the cloud is encrypted at rest in GCP (Google Cloud Platform).
- All connections to PaperCut Cloud Services use TLS to encrypt data in transit (by default, TLS 1.2+ with perfect forward secrecy (PFS)).
- Print jobs stored on premises at rest in the Edge Mesh are encrypted using AES-256 GCM.
- The last step of the print process, from the Edge Mesh to the printer, is limited by the level of encryption the printer supports; when available, TLS is used.

Does PaperCut audit its cloud security?

PaperCut has an extensive security program that includes ongoing testing of our cloud-hosted systems and products. The program includes independent third-party assessment in the form of penetration testing (White Box, Code-Assist, and Threat-based). PaperCut also has a Security Vulnerability page that covers all our cloud products.

Do you make your security testing results available?

Yes, on request we are happy to make available the results of our last third-party penetration testing (White Box, Code-Assist, and Threat-based).

The results are available in a summary document or, on a case-by-case basis, and under NDA. We can make available the full results of the last penetration test, including full disclosure of any issues found and their remediation status.

To access these reports, lodge a ticket with PaperCut Support through our Support Portal, and mark it “Attention to the PaperCut Security team.”

Does PaperCut have a security incident response plan?

Yes. When an incident occurs our Incident Response Plan is executed by our Incident Response Team.

Does PaperCut have backups?

Yes, PaperCut Pocket and PaperCut Hive data is backed up daily. Data is also duplicated within multiple zones in the region in which it is located.

Note that not all data is backed up, as some data is transient and governed by strict lifecycle rules (for example, print jobs stored in the Cloud Node or in scan jobs waiting for delivery). As soon as the jobs are delivered, the data is permanently deleted. This minimizes the period in which we retain potentially sensitive data. All activity in the PaperCut system (such as print jobs, scan jobs, administrator audit behavior, and configuration data) is always retained and backed up until an approved administrator requests for an organization's account to be deleted.

How is my data separated from other PaperCut customers' data?

Data separation is fundamental to the design of a secure multi-tenanted system.

Because PaperCut Pocket and PaperCut Hive were developed to run in a multi-tenant, built-for-cloud environment, we have chosen modern security patterns that are used by major cloud players.

Under the hood, PaperCut runs on Google Cloud services, and data tenancy features are always used where possible.

One of the fundamental concepts is the extensive use of namespaces. Each organization has a unique ID assigned (referred to as an Org ID). All requests to the PaperCut Cloud Service must present a signed authentication token that contains the same Org ID so the request can be authorized.

Also, data tenancy is an actively tested area in our third-party penetration tests.

Is the PaperCut cloud infrastructure secure?

PaperCut's cloud infrastructure runs in Google Data Centers. Google handles the physical security; the application-level security is actively monitored for security events by PaperCut using Google's built-in security monitoring.

Only authorized PaperCut employees have access to the cloud infrastructure and the ability to deploy a code change. MFA (Multi-Factor Authentication) is a requirement for all PaperCut employees and is enforced on all cloud infrastructure access.

When customers access PaperCut Pocket or PaperCut Hive, how are authentication and authorization handled?

PaperCut Pocket and PaperCut Hive administrative authorization is implemented using the OAuth2.0 standard. SysAdmins have a choice of authentication providers: Google, Microsoft, or PaperCut (username and password). Both Microsoft and Google offer MFA (Multi-Factor Authentication) options and PaperCut recommends you enable them.

For print release, end-user authentication is authorized by email.

Will PaperCut let me know if there is a security incident?

In the very rare event that a security incident occurs that impacts you or your organization, we'll notify you in line with regional reporting requirements and laws. We understand that timely notifications will allow you to take steps to reduce the potential harm due to the incident.

PaperCut complies with all applicable laws and/or rules about mandatory disclosure of breaches or incidents involving personal information.

We also recommend signing up for our Security Notifications.

Is PaperCut certified against any of the major security standards – for example, SOC II/III or ISO 27001?

PaperCut is currently in the process of getting ISO 27001 certification.

Can PaperCut employees view my print job data?

We can't see what we don't have. PaperCut Pocket and PaperCut Hive don't have access to print jobs that are printed when the Cloud Node is disabled. In this case, the contents of the print jobs remain in the Edge Mesh and are deleted immediately after they have been printed. If the Cloud Node is enabled, the print jobs are saved in PaperCut Pocket and PaperCut Hive and are automatically deleted after 72 hours or immediately when they are printed. Only authorized PaperCut employees have access to print job data saved in the cloud infrastructure.

Does my print job data leave my premises?

You have complete control over when your print jobs' contents remain on your premises. If the organization has enabled Cloud Node and the document is printed remotely or needs to be routed to a remote location, the document will leave the premises.

Summary information about the print job is sent to the cloud. The information includes a thumbnail of the first page (if enabled), the name of the user who printed it, the document name, and general print attributes such as paper size, the number of pages, and two-sided settings. We also send IP addresses associated with edge nodes and printers.

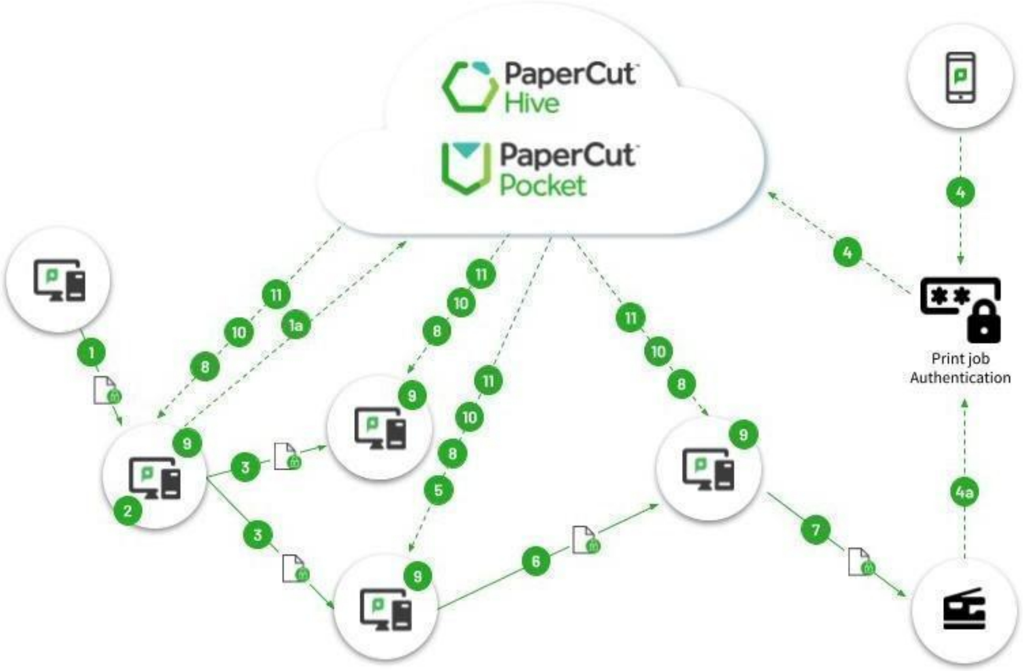
All this information is secured using the practices outlined in the next section.

Where does my document go when I print?

We want you to be in charge of where your print jobs go. Document flows are different depending on how PaperCut is configured in your organization. Read below for a description of the flows for the following scenarios:

- Default Print Release (only standard edge nodes)
- Print release via the Cloud Node
- Print Release when a SuperNode is enabled

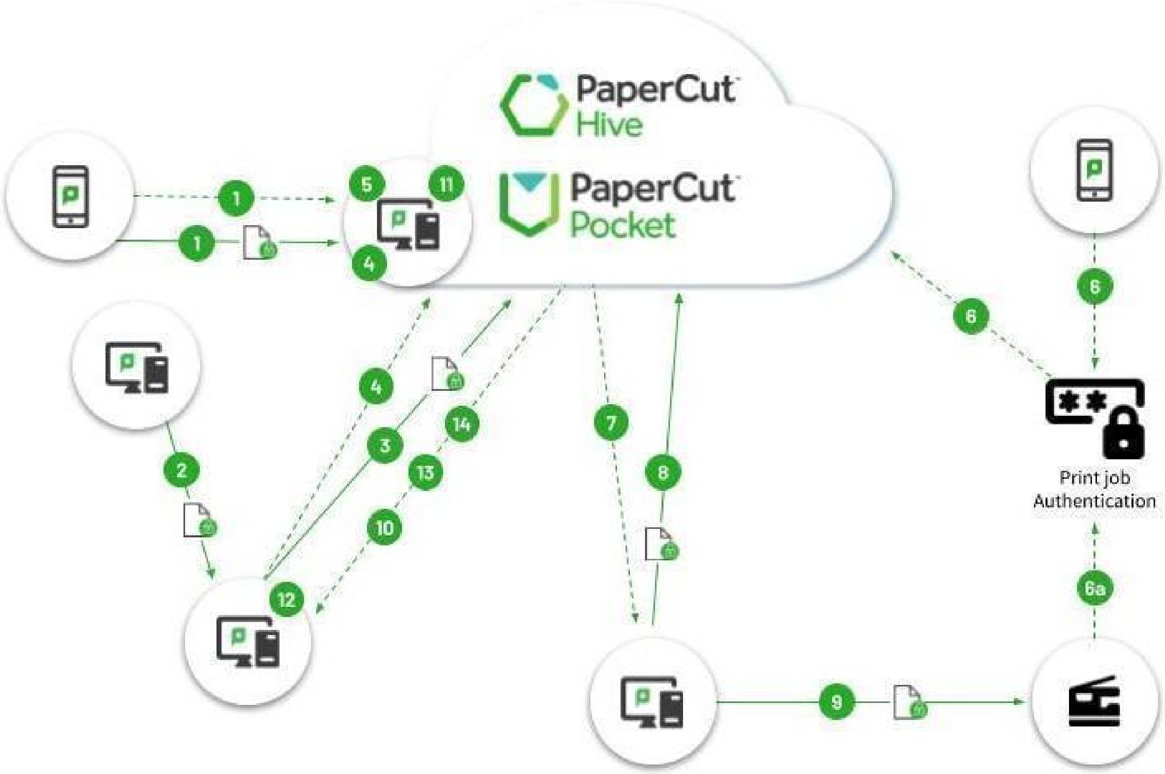
Default print release (only standard edge nodes)



1. When the job is submitted by the user, it is transmitted to an edge node via TLS.
2. The edge node sends the Job Metadata to PaperCut Hive or Pocket using TLS.
3. The edge node processes the document using temporary storage. Once processed, the edge node encrypts the document and saves it to disk.
4. The initial edge node replicates the document to other edge nodes via TLS. Each subsequent edge node encrypts the document before saving it on disk.
5. The user releases the job for printing using either the Mobile App or the MFD. (Note, MFD Release is only available for PaperCut Hive, not PaperCut Pocket.)
6. When the job is released, PaperCut Hive or Pocket notifies an edge node to send the job to the printer.
7. If none of the edge nodes that hold the print job have access to the requested printer, the job is routed to an edge node that can access the printer.
8. The edge node encrypts the job and sends it for printing either via IPP or a local queue. The connection to the printer uses the highest level of encryption supported by the printer configuration on that device.
9. After the document has been printed PaperCut Hive or Pocket is notified, then PaperCut Hive/Pocket notifies all edge nodes that have saved the document to delete it.

10. If an edge node is offline, it will delete a document after 72 hours or the next time the system is powered on after the timeout has expired. This timeout is configurable for up to 96 hours.
11. If a document is not released, PaperCut Hive or Pocket will notify edge nodes to delete the document after the document timeout elapses, which defaults to twelve hours.
12. If a user cancels the print job, the document is deleted from edge nodes.

Print release via a Cloud Node



1. When the Cloud Node is active, all print jobs are replicated in the cloud.
2. When a user prints a job and their computer's print client can't find a reachable edge node (this usually occurs when the client is a Chromebook or Android), the client will submit the job, including metadata, directly to the Cloud Node using TLS.

   Notes:
   - With iOS, if the user selects a Cloud Node from the Printer list, the job is sent to the Cloud Node regardless of the presence of reachable edge nodes.
   - Due to limitations with iOS printing, TLS Certificates aren't validated on the Connection to the edge node.
3. If a Print Client can find a reachable edge node, the print job, including metadata, is sent to that node.

4. If the initial edge node cannot replicate to another local edge node, it replicates the print job to the Cloud node instead.
5. If the Cloud Node is the first node to receive the print job it submits job metadata to the PaperCut Hive or Pocket. Otherwise, the initial edge node sends the job metadata to PaperCut Hive or Pocket.
6. Once a job is replicated to the Cloud Node, it's encrypted at rest using default Google encryption.
7. The user releases the job for printing using either the Mobile App or the MFD. (Note: MFD release is only available for PaperCut Hive, not PaperCut Pocket.)
8. PaperCut Hive or Pocket notifies an edge node to request the job.
9. The releasing edge node downloads the print job from the cloud using the signed URL.
10. The edge node sends the job for printing via either IPP or a local queue. The connection to the printer uses the highest level of encryption supported by the printer configuration on that device.
11. After the document has been printed, PaperCut Hive or Pocket is notified. PaperCut Hive or Pocket then notifies all edge nodes that have saved the document to delete it.
12. The Cloud Node deletes the job on print or after 72 hours if it is not printed.
13. If an edge node is offline, it will delete a document after 72 hours or the next time the system is powered on after the timeout has expired. This timeout is configurable for up to 96 hours.
14. If a document is not released, PaperCut Hive or Pocket will notify edge nodes to delete the document after the document timeout elapses, which defaults to twelve hours.
15. If the user cancels the print job, the document is also deleted from edge nodes.

Print release when a SuperNode is enabled

1. When an edge node is promoted to a Super Node, that node becomes a priority destination for print jobs for all print job transmission, including print release, print job submission, and job replication. Note: With iOS, the only edge nodes that appear in the Printer List are Super Nodes and Cloud Nodes.
2. Otherwise, the behavior is as above in either default mode or when there is Cloud Node Enabled.

How can I get more information on security?

We love chatting and feedback! If you have any further questions, please reach out to us via your reseller or send a question to us via https://support.papercut.com.