

Windows Protected Print Mode (WPP)

info icon

Should I switch on WPP now?

Not yet! PaperCut is actively working on a solution to support printing with Windows Protected Print Mode. Sign up for early access through our [Percolator program](#).

What is Windows protected print mode?

Windows protected print mode (WPP) is a security-enhanced printing platform for Windows that runs with lower privileges and uses Internet Printing Protocol (IPP) to eliminate the need for third-party drivers. Together, these remove significant security risks that can lead to attackers gaining SYSTEM-level access.

Whether you're an IT manager, security professional, or business owner, understanding the impact and benefits of WPP is essential as it changes the landscape of print infrastructure. This page provides a comprehensive overview of WPP, its timeline, and how your organization can prepare for and benefit from this powerful security feature.

Why Microsoft is introducing Windows Protected Print Mode

[According to Microsoft](#), 9% of Windows security issues reported to the Microsoft Security Response Center (MSRC) were caused by print stack-related issues. The fact that the spooler runs with system privileges and has to load code over the network makes the entire operating system vulnerable to malware.

[Print Nightmare](#) allowed hackers to exploit this vulnerability to install programs remotely, view and delete data or even create new user accounts with full user rights. Another spooler-related weakness was exploited by the Stuxnet virus, which was used as a digital weapon to [gain remote access to the computers](#) that controlled centrifuges at an Iranian uranium enrichment plant. This allowed the attackers to configure the fast-spinning centrifuges to tear themselves apart.

Print Nightmare patches are a temporary workaround that now requires admin rights to install printers. The admin rights requirement only protects a shared computer, where one user might have installed a printer driver with malware that would compromise others on the computer too. This change doesn't fix the spooler privilege issue that is exploitable by a driver with malware, and it introduces user experience issues by forcing admin privileges just to install printers.

The proper solution is Windows Protected Print Mode, as it removes the fundamental flaw of drivers and moves the world of printers forward to finally settle on the IPP standard. At PaperCut, we support Microsoft's decision, even though it will cause some adoption friction.

As an aside, Windows isn't the only operating system plagued by a vulnerable print platform. CUPS, used in Linux, macOS, and ChromeOS, also has a long history of security issues. In September 2024, new reports showed how it is [possible to remotely execute code on a Linux computer](#) without requiring authentication. Some Linux distributions, like Ubuntu, are planning to limit access to the rest of the operating system by moving CUPS into a containerised Snap App.

How Windows Protected Print Mode works

WPP uses modern standards and secure communication methods to ensure a robust and consistent printing experience. Here are some of the key details.

1. Printer and job delivery is based on Internet Printing Protocol (IPP)
 - WPP uses IPP as the core transport protocol - a well-established, open standard that provides a framework for printer discovery, job submission, and status tracking.
 - IPP allows WPP to support advanced features such as finishing options, job status updates, and access control, enabling a richer printing experience.
 - The port monitor used when adding a WPP print queue is Microsoft's new IPP port, which provides a richer set of IPP functions.
2. No more third-party printer drivers and modules
 - WPP forces a driverless printing model. When it's enabled, client computers can no longer load third-party printer drivers, eliminating the risk of attackers loading malicious code.
 - In addition to the printer drivers, the loading of other, less well-known modules, such as third-party [print providers](#), is blocked.
 - WPP prevents Point and Print from ever installing third-party printer drivers. This eliminates the risk of an attacker pretending to be a printer and tricking users into installing malicious software.
3. Common print spooler tasks are now run at lower privilege level
 - Since the drivers are no longer required to run as SYSTEM, most common spooler tasks can now run as USER.

- This reduces the risk of a rogue or a buggy program taking down the whole machine. The impact will be limited to actions only the user can perform.

The challenges of transitioning to Windows Protected Print Mode

When you switch on Windows Protected Print Mode, the existing print queues and drivers on the computer will be permanently deleted. You won't get them back if you decide to switch WPP off. It is an all-or-nothing setting.

You can't use a driver for some printers while using Windows Protected Print Mode for others. If WPP is enabled, print drivers are nonexistent.

Not all printers are equal. Based on a sample of thousands of printer models we assessed, roughly 70% of printers will work seamlessly over IPP. For the rest, they will either function with reduced speed, lower quality or not at all.

Existing scripts that system admins may have in use, such as [printui](#) scripts to manage printers, won't work anymore.

How enabling WPP will affect organizations and their print infrastructure

To understand how enabling Windows Protected Print Mode might affect organizations, let's use a hypothetical scenario:

info-green icon

Info

“

The university IT administrator's dilemma

Alex, the lead IT administrator at a mid-sized university, heard about WPP during a recent security conference.

The idea of having a more secure, driverless printing environment using the Internet Printing Protocol (IPP) sounded like a great way to tighten the university's security. With hundreds of devices across different departments, ensuring that no vulnerabilities could be exploited through outdated drivers or unmonitored print processes seemed like a major win.

Eager to implement WPP, Alex decided to enable it across the university's network, confident that this would reduce risks and future-proof the printing setup. The change went live during a routine maintenance window, with IT teams monitoring performance and response.

However, as the next day began, emails started flooding in from staff and students across campus. The university's fleet, consisting of older and newer printers, faced a serious issue: **30% of the printers weren't working!** Despite being reliable for everyday use, they weren't Mopria compliant and/or IPP-compatible.

The Issues staff and students were experiencing

1. Printer Recognition Problems: Some of the older printers weren't showing up in Windows' printer lists anymore and attempts to manually add printers were failing with error messages "can't add"
2. Loss of Features: Other printers were partially working, but features like stapling, colour management, and even advanced security protocols like pull printing were no longer functional. This disrupted the workflows of departments that relied heavily on advanced printing tasks.
3. User Frustration: Professors were missing critical deadlines to print exams, and research departments couldn't print their reports. The more Alex's team tried to patch things up, the more they realised the issue was systemic: these printers did not support IPP and were reliant on specific drivers that WPP no longer allowed.

Lessons learned

In retrospect, Alex realized that turning on WPP without fully assessing the fleet was premature. **While the security benefits were undeniable, it required careful planning and implementation.**

Will my printer work with Windows Protected Print Mode?

Mopria has an [online list of certified printers](#) you can use to check your printer models.

Although a printer could be listed as Mopria-certified, it doesn't necessarily mean it will work with WPP or that you will get the most out of your printer once you switch over to using IPP in WPP mode.

At the time of writing, Windows Protected Print Mode deems some IPP attributes mandatory, even though they are technically specified as optional according to Mopria standards, such as the hardware ID. Additionally, WPP requires some IPP values to be in a specific format that some printers do not follow.

Some printers that support IPP don't necessarily support PDF-based spool files; instead, they only support formats like URF/raster or JPEG. This still follows the specification, but these spool files will be much larger and often print in lower quality. In addition to being larger, these formats require the entire print job to be submitted to the printer before the printer can start printing them, which results in slower printing or even failure to print larger documents as the printer can't store the entire print job.

For now, the best way to confirm that your printer is ready for WPP is to enable WPP on a test Windows machine and print from it. If your printer can't be found when WPP is enabled, you know it's incompatible.

Check different finishing options, especially more advanced options like stapling and tray selection if the printer supports it.

Options for printers that are non-compliant with Windows Protected Print Mode

We are making changes in PaperCut MF/NG and PaperCut Hive/Pocket to support printers that are WPP ready and also printers that are not WPP ready. You can [sign up for PaperCut MF/NG Early Access](#) now. PaperCut Hive/Pocket Early Access registrations will open in November.

Alternatively, if your printers are not ready, your printer manufacturer may soon provide a firmware update if your printers are not too old, so keep an eye out.

How to switch on Windows Protected Print Mode

Enable WPP mode via Settings

How to enable WPP on your computer

1. Navigate to Settings > Bluetooth & devices > Printers & scanners > Printer preferences

papercut WPP navigate to Settings > Bluetooth & devices > Printers & scanners > Printer preferences

2. Click 'Set Up'. Windows will display a warning message.

papercut WPP Click Set Up Windows will display a warning message.

3. Additionally, if WPP-incompatible print queues (such as standard TCP/IP queues) were already installed, Windows would warn that they would be removed.

papercut wpp warning

4. After successful completion, WPP should be turned on.

papercut WPP should be turned on

Enable WPP mode via Group Policy

Via Group Policy Editor > Administrative Templates > Printers > Configure Windows protected print > Edit

papercut wpp group policy approach

Timeline and updates

Note that these dates are subject to change:

01 OCTOBER 2024

When you enable Windows Protected Print Mode for the first time after the 24H2 upgrade, the existing incompatible (such as TCP/IP) queues may not get deleted. Also, you may still be able to

create TCP/IP print queues. A system reboot may fix the issues. This is a known issue, and Microsoft is working on fixing it.

04 OCTOBER 2024

Microsoft is pushing the patch [KB5043178](#) to fix Windows protected print anomalies soon. The estimated rollout date is 8th October.

NOVEMBER 2024

First PaperCut MF/NG Windows Protected Print Mode release planned.

JANUARY 2025

First PaperCut Hive/Pocket Windows Protected Print Mode release planned.

2027

Windows Protected Print Mode is enabled by default.

Further reading

- The official [Microsoft Windows Protected Print Mode announcement](#)
- [More from Microsoft about WPP](#)
- Microsoft's [Windows protected print mode FAQ](#)

Revision #1

Created 24 October 2024 12:49:49 by joliveira

Updated 24 October 2024 12:50:05 by joliveira