MPSA
MANAGED PRINT
SERVICES ASSOCIATION

MPSA Windows Protected Print eBook

Standards and Best Practices
February 2026

The MPSA definition of Managed Print Services (MPS):
"Managed print services is the active management and optimization of business processes related to documents and information including input and output devices."

Internet:	http://www.yourmpsa.org
Follow us on LinkedIn:	www.linkedin.com/company/mpsa/
Subscribe on YouTube:	www.youtube.com/@yourmpsa

MANAGED PRINT SERVICES ASSOCIATION

The MPSA is the only international, independent and nonprofit MPS organization that embraces all industry participants in a collaborative environment. The MPSA is NOT owned or directed by any one organization; it is in fact owned by its members. The influence of any single company, large or small, is prevented by the MPSA charter.

Our Mission

The mission of the MPSA and its members is to address and optimize businesses’ office document management while enhancing the growth, efficiency, and profitability of the MPS segment through advocacy, marketing, education, research, standards, and a general community of interest.

In order to reach these objectives, the MPSA provides community-driven best practices—like those contained in this eBook — to empower its members to make more informed decisions regarding their MPS strategies.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Presented by the Standards and Best Practices Committee

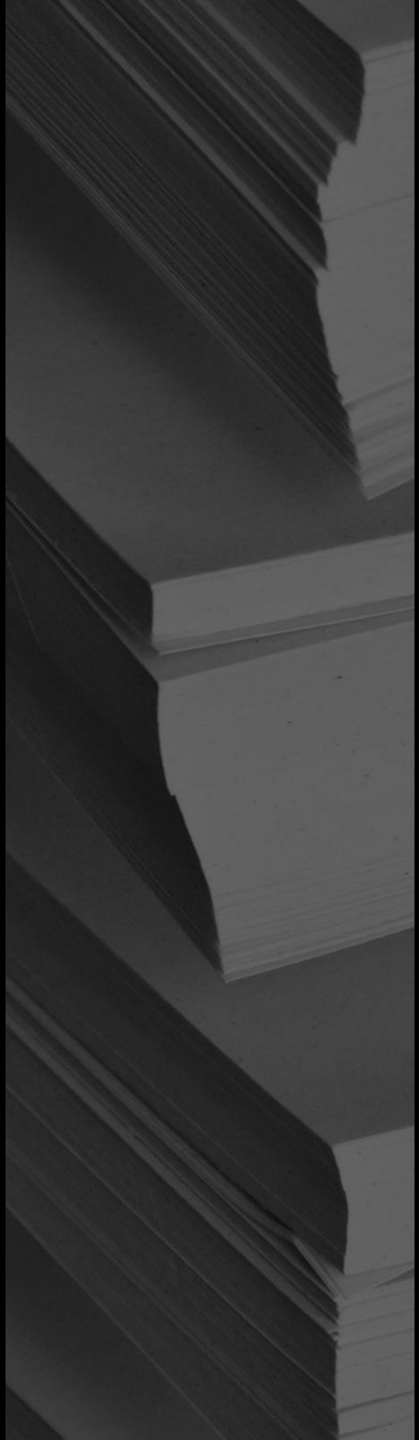
Contact: standards@yourmpsa.org

Content Input:

- Eric Crump, RINGDALE
- AJ Reisinger, Exela Technologies
- Nick Hienton, imageOne
- Robert Palmer, IDC
- Will Parker, Datasec Solutions
- Steve Inch from HP

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Introduction



Organizations looking to implement Microsoft Windows Protected Print are navigating new opportunities for enhanced document security and print management. As adoption grows across enterprise, education, healthcare, and government environments, clear and consistent terminology becomes critical for smooth implementation, support, and collaboration.

Windows Protected Print Mode Timeline

- **2024 (Win11 24H2):** WPP introduced as optional.
- **2025:** Microsoft stops accepting new third-party drivers.
- **2027:** WPP expected to become the default print mode.

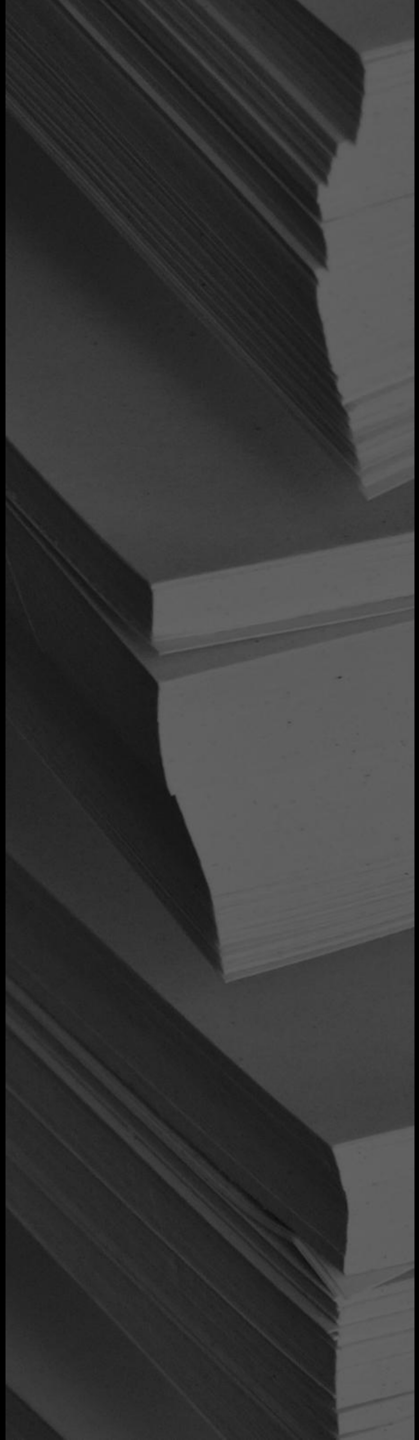
To assist with this, the MPSA Standards and Best Practices Committee has developed this vendor-neutral reference guide defining key details and terminology related to Microsoft's Windows Protected Print.

This eBook is designed to help IT teams, managed print providers, and end users communicate more effectively and consistently as they plan, deploy, and manage secure printing within the Windows ecosystem.

And a special thank you to all the volunteers of the MPSA that made this reference a reality. Without our volunteers, there isn't an MPSA. We ask any reader of this eBook to consider becoming a volunteer with one or more committees with the MPSA.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Windows Protected Print Reference



What is Windows Protected Print?

Representing one of the largest changes to the Windows print system in over 20 years, Windows Protected Print (WPP) mode is designed to transition Windows print from legacy v3 and v4 print drivers to modern driverless printing using Internet Printing Protocol (IPP).

What prompted this change?

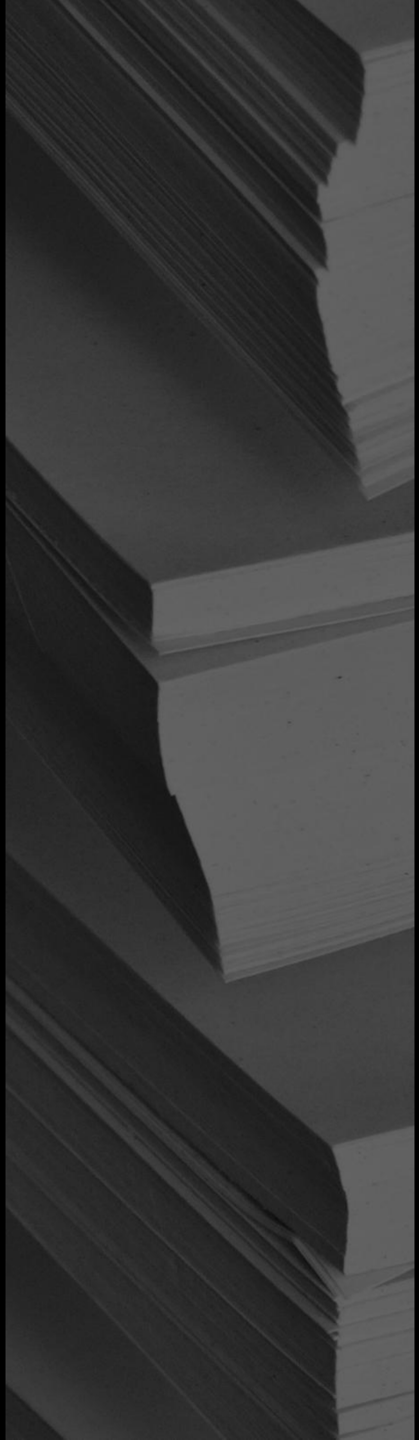
Since Print Nightmare, Microsoft has been working to modernize the Windows Print System. This new design represents one of the largest changes to the Windows Print stack in more than 20 years.

Microsoft says that one of the largest motivations behind the change is security. The Windows print system has recently been a key target for attackers. Print bugs played a role in Stuxnet and Print Nightmare, and account for 9% of all Windows cases reported to the Microsoft Security Response Center.

Securing the print stack is challenging, in large part due to the use of third-party drivers. WPP is a response to this situation.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Windows Protected Print Reference



Microsoft view of security Issues in Legacy Printing

Drivers

- Security model relies on shared responsibility between Microsoft and vendors
- Loading code from third parties is a security challenge, as vulnerabilities are vendors’ responsibility to fix
- Discrete drivers for older printers may not have been updated for years
- Although V4 driver architecture was introduced in 2012 most drivers in use are still V3
- Flexibility of V3 drivers forces compromises as customers want printing to be as painless as possible

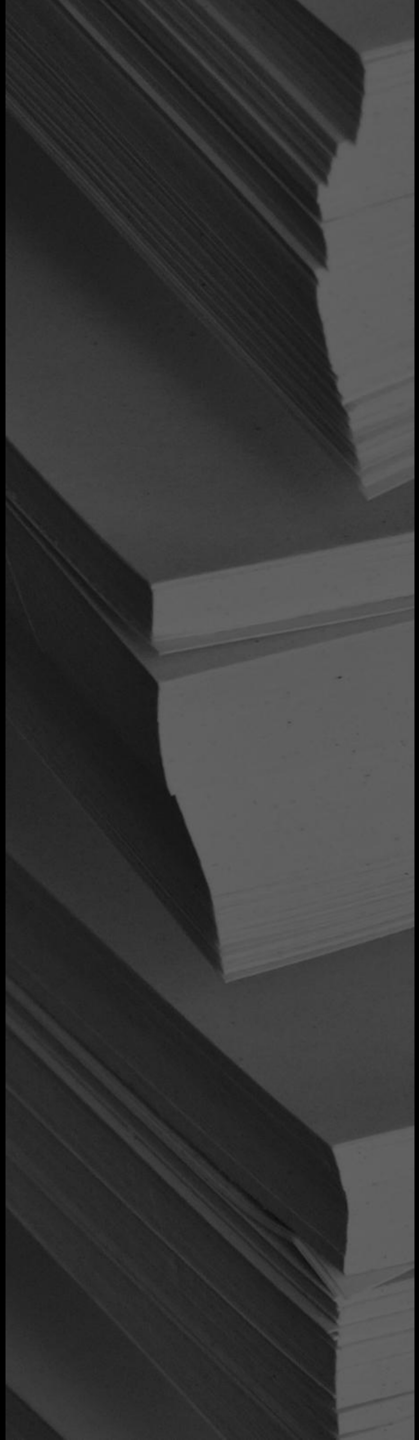
Compatibility

- Some legacy drivers are incompatible with modern security mitigations (e.g., CFG, CET, ACG) and have not been updated by manufacturers

Excessive Permissions

- Bugs can lead to full spooler control as print drivers run as SYSTEM with full privileges, for example Print Nightmare authentication vulnerability

Windows Protected Print Reference

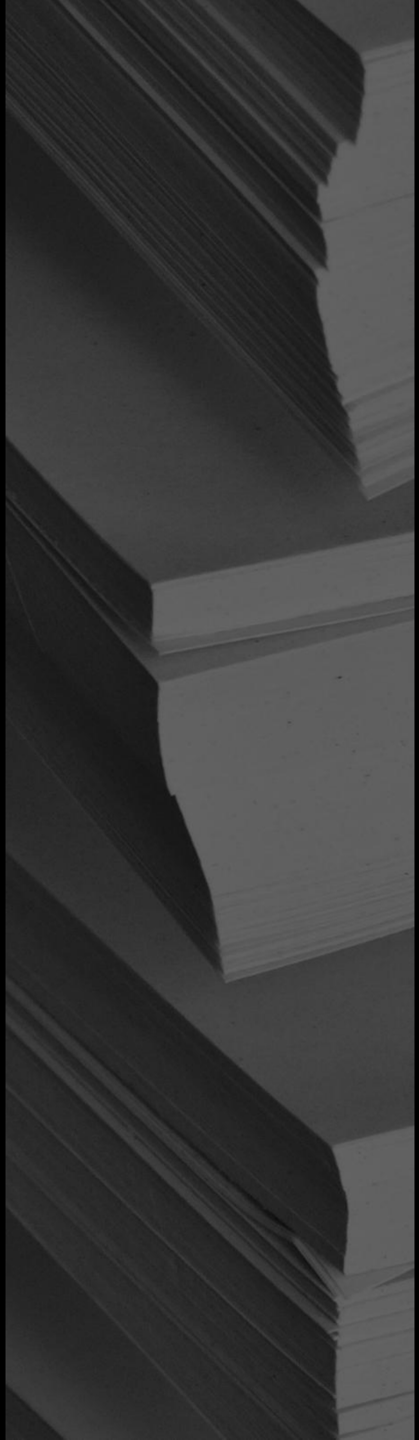


What should the replacement be to Legacy Printing?

Luckily, a secure alternative already exists.

- Internet Print Protocol (IPP) is based on well-known secure protocols
- IPP supports all common operations expected of printing functions
- Driverless printing reduces code complexity and enables client-side rendering
- IPP printing is already part of Windows and works with Mopria-certified printers
- The Mopria Alliance is an Industry group providing IPP-based universal standards and solutions for print and scan
- Most printers introduced since 2012 are Mopria certified
- Every other major operating system developer has already implemented IPP (Apple, Google, Linux etc)

Windows Protected Print Reference



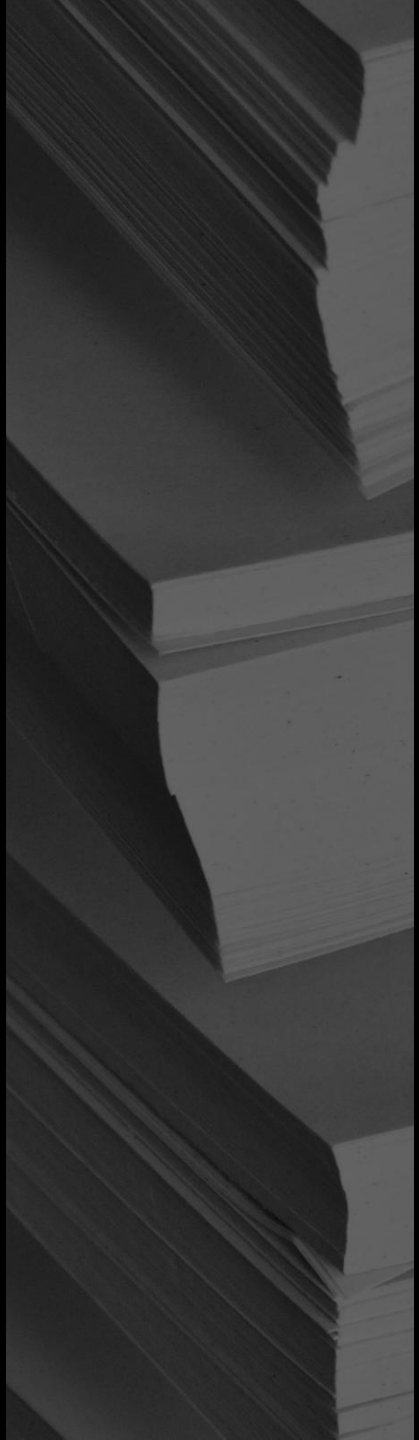
A Transition to Windows Protect Print Mode

- Windows Protected Print mode (WPP) is part of a multi-year plan to move the "legacy" Windows print subsystem to an IPP-based architecture

- **2024 (Win11 24H2):** WPP introduced as optional.
- **2025:** Microsoft stops accepting new third-party drivers.
- **2027:** WPP expected to become the default print mode.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Windows Protected Print Reference

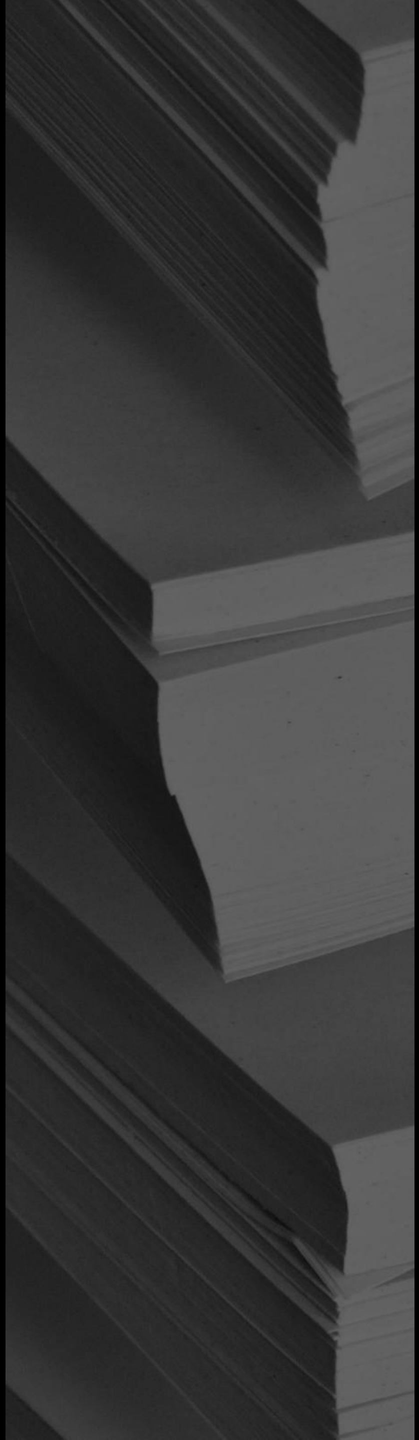


Windows Protected Print Mode changes

- **Limited Print Configuration**
  Restrictions on print ports and legacy APIs
- **Module Blocking**
  Only MSFT-signed binaries required for IPP are permitted
- **Per-user rendering**
  XPS rendering runs as user instead of SYSTEM
- **Security mitigations for binaries**
- By only using MSFT binaries, the use of modern mitigations such as CFG, CET can be used by developers
- **Point and Print**
  Restricted from installing non-MSFT drivers
- **Transport security**
  WPP will show print traffic encryption status and encourage use of encryption

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

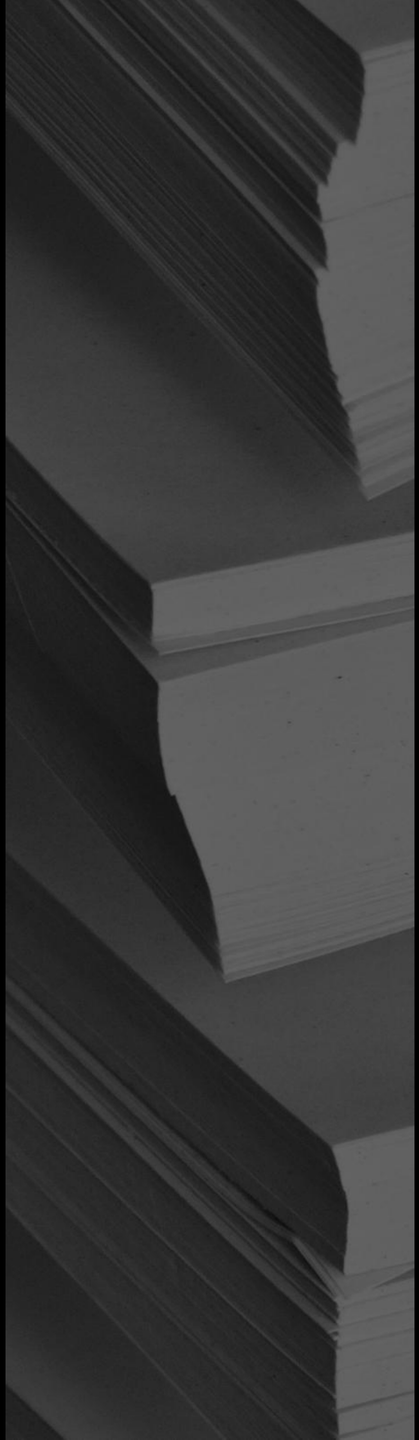
Windows Protected Print Reference



Detailed WPP behaviour changes

- In October 2024 Windows Protected Print (WPP) was released via Windows update (though not enabled by default on W11 24H2) and will be included in Server 2025
- MSFT intent is to change the default in future releases of Windows to WPP being enabled by default
- When WPP is enabled on Windows, all V3 and V4 print, and scan driver objects are deleted and only IPP queues can be created
- Once enabled, WPP can be changed back to “Not Enabled”, allowing the installation of V3 & V4 drivers and associated queues again but will not restore previous drivers and queues
- Printers discovered by WSD or “Add Printer Wizard” will have queues created using the MSFT Inbox IPP Class Driver which has limited functionality compared to vendor drivers

Windows Protected Print Reference

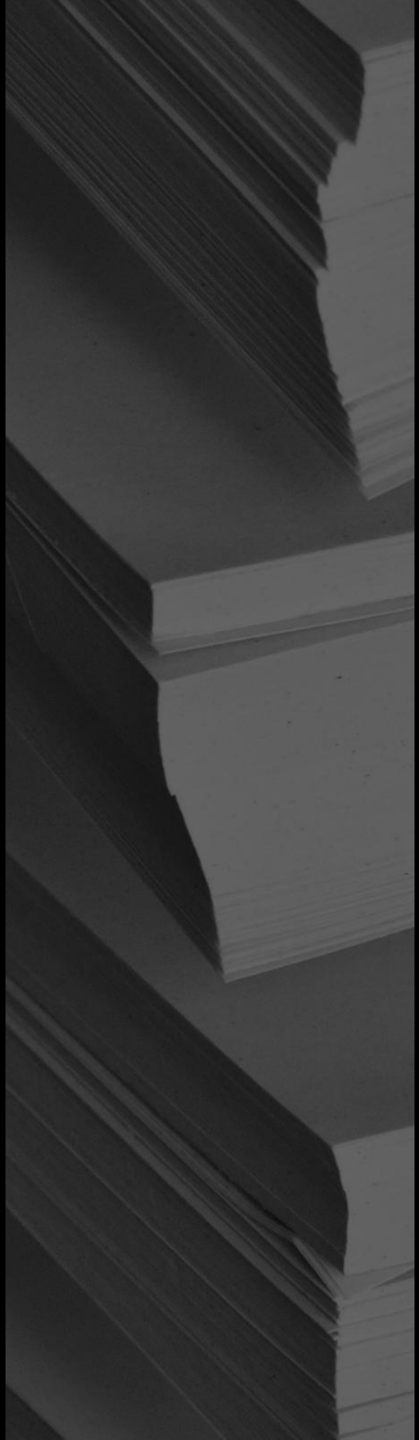


Print Support App (PSA) - Customized Windows IPP Class Driver capabilities

- MSFT planned replacement for print workflows which require a customized experience is the Print Support App (PSA)
- PSA is a MSFT-developed technology for developers, allowing features provided by traditional V3 & V4 drivers to be available to devices using the IPP class driver
- A PSA does not require WPP, but WPP requires a PSA for a customized experience

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Windows Protected Print Reference



Print Support App (PSA)

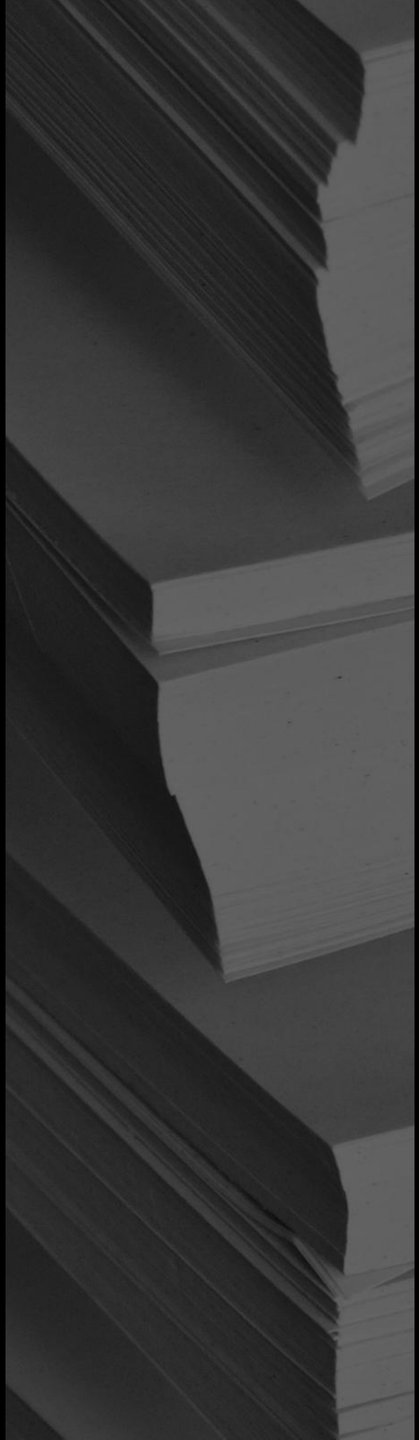
What is PSA

- Microsoft’s latest Mopria IPP-class, app-based driver solution designed to streamline & enhance the print experience
- Key aspect of Microsoft’s long-term driver support strategy, and the broader evolution in print technology, towards a cloud-based, user-friendly solution

Key Features

- Ability to build a consistent, simplified, customizable user experience across the enterprise print portfolio
- Designed with cloud capabilities, enabling features like remote printing and integration with OEM, ISV, and MSFT print cloud services
- Built with the latest security protocols, PSA ensures secure printing and data handling, aligning with modern cybersecurity standards

Actions and Next Steps



Audit Your Customers' Environments

- Identify which devices rely on vendor-specific drivers and whether they support IPP Everywhere / Mopria / Universal Print.
- Flag devices that don't support IPP, as these will lose print functionality under WPP.2.

Engage Vendor Roadmaps

- Meet with OEM partners (HP, Ricoh, Canon, Xerox, etc.) to confirm their PSA (Print Support App) availability and certification timeline.
- Ask how they plan to support MICR printing, finishing, fax, and scan features under WPP.3.

Pilot Early

- Enable WPP in a controlled test group to identify compatibility or workflow issues.
- Test both print and scan workflows, including secure release and accounting integrations.

Update Print Management Solutions

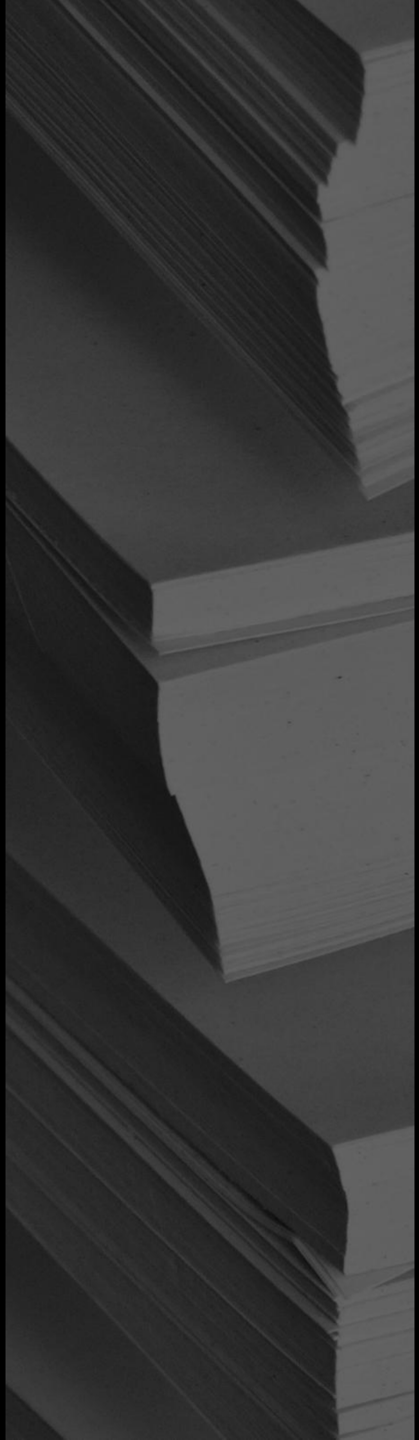
- Ensure your print management platform supports IPP printing and WPP-aware workflows.
- Vendors are beginning to roll out WPP-compatible connectors and Universal Print integrations.

Educate IT Teams and Users

- Train staff on driverless printing, Universal Print registration, and PSA deployment through the Microsoft Store or Intune.
- Emphasize that traditional "point-and-print" installs are no longer allowed.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Windows Protected Print Terminology



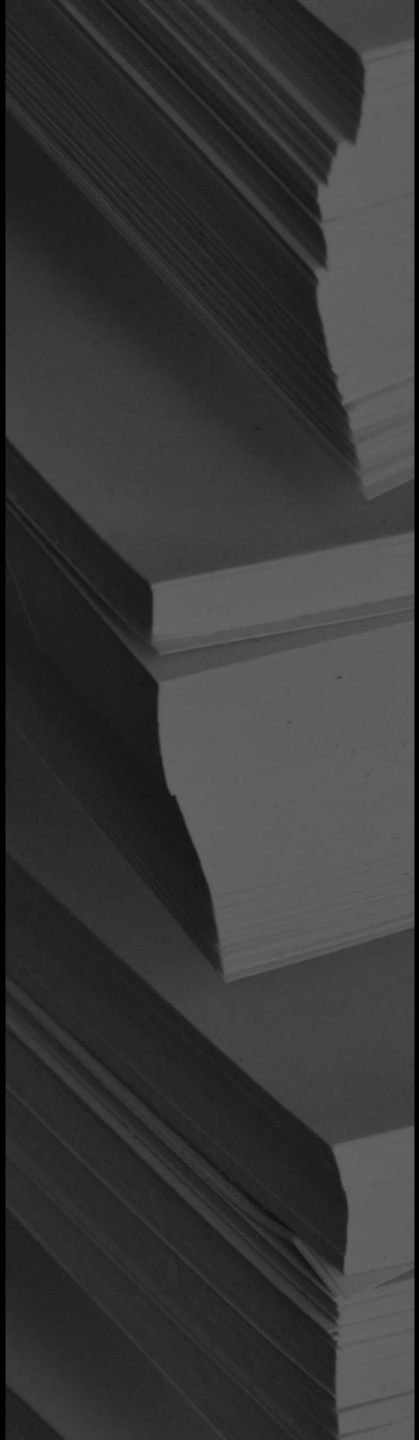
This list of terminology is the top list to be aware of, and it is not an exhaustive list. MPS providers should reflect on these terms as minimum recommendations in their MPS offering to prospective buyers.

This eBook is a collaboration led by the Standards and Best Practices Committee and has been reviewed and approved by MPSA members and industry experts.

Readers of this eBook can provide direct input regarding the report to standards@yourmpsa.org to be considered for future amendments or additional educational formats like live stream events or blog articles presented by the MPSA.

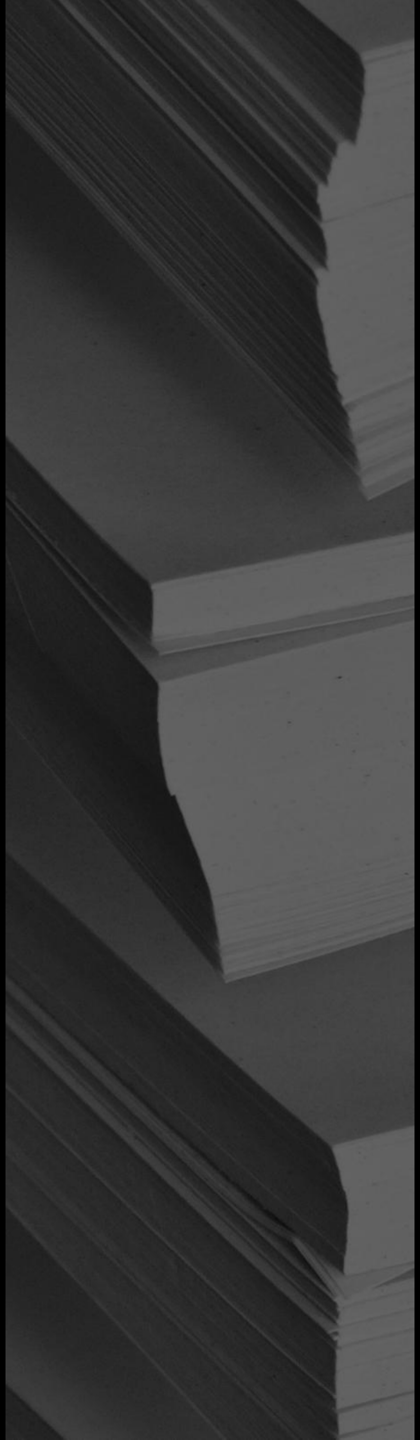
MPSA
MANAGED PRINT
SERVICES ASSOCIATION

WPP Terms



1. WPP (Windows Protected Print)
2. IPP (Internet Printing Protocol)
3. IPP Class Driver
4. V3 Driver
5. V4 Driver
6. Point and Print
7. Print Spooler
8. PrintNightmare
9. Print Support App (PSA)
10. Mopria
11. Fax Printer
12. XPS (XML Paper Specification) Printer
13. Secure Printing
14. Driverless Printing
15. Zero Trust Printing
16. Microsoft Universal Print
17. Entra ID
18. Zero-Day Vulnerability or Attack

WPP Terms



1. **WPP (Windows Protected Print):**

   Microsoft's new secure print mode in Windows 11 that eliminates third-party printer drivers and enforces security through IPP Class Drivers.

2. **IPP (Internet Printing Protocol):**

   A standardized, driverless printing protocol used by WPP to communicate with printers.

3. **IPP Class Driver:**

   The built-in, universal Windows print driver that supports IPP printing; replaces manufacturer-specific drivers under WPP.

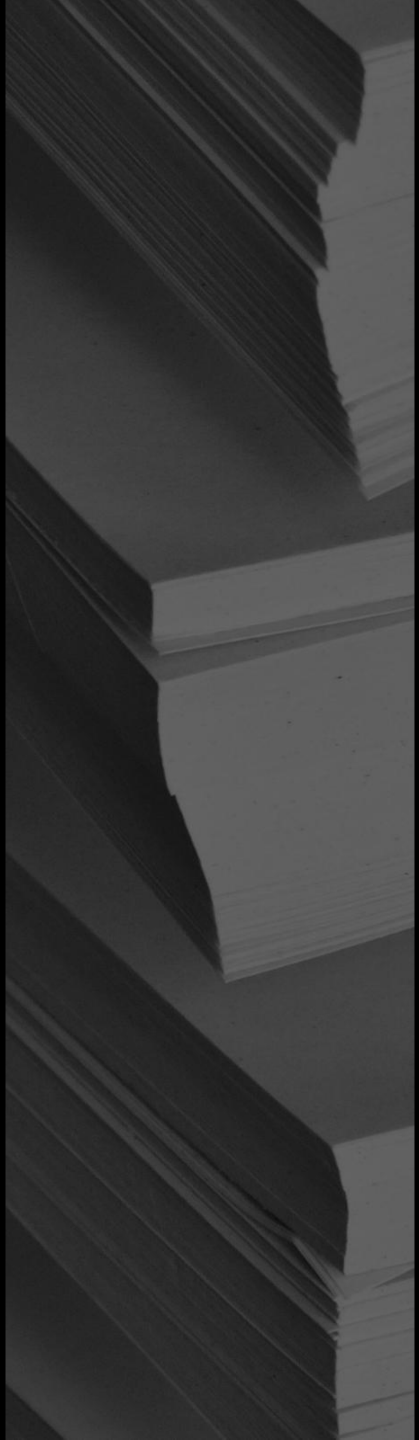
4. **V3 Driver:**

   Traditional printer driver model used in older versions of Windows; not supported under WPP.

5. **V4 Driver:**

   Modern driver model introduced in Windows 8; also not supported under WPP.

WPP Terms



6. **Point and Print:**

   Windows feature that allowed automatic installation of printer drivers from a server; disabled in WPP for security.

7. **Print Spooler:**

   Windows service that manages print jobs; WPP runs it with lower privileges to reduce vulnerabilities.

8. **PrintNightmare:**

   A critical 2021 Windows print spooler vulnerability that prompted Microsoft to create WPP.

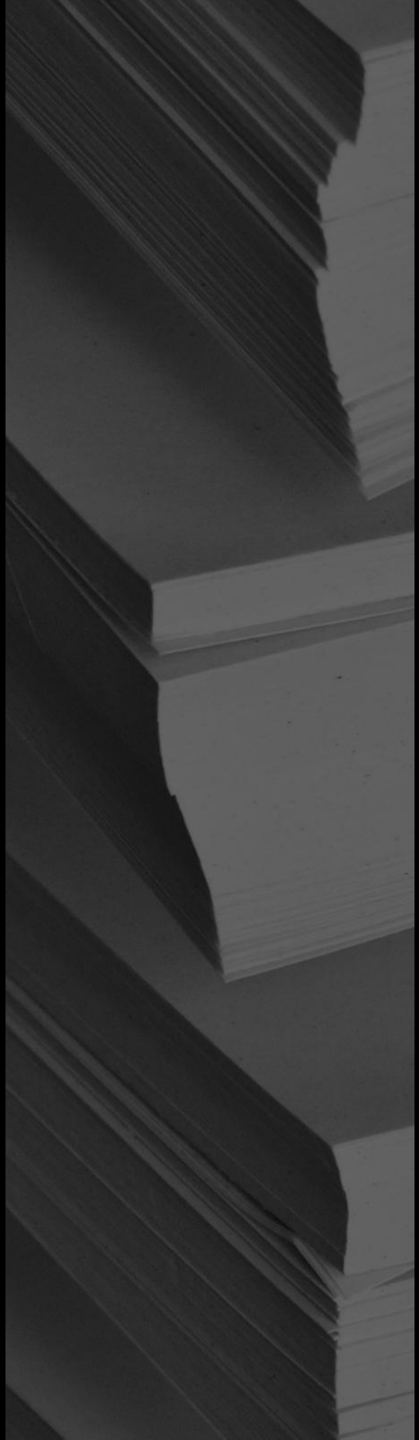
9. **Print Support App (PSA):**

   Microsoft's app-based architecture that printer vendors can use to deliver advanced features (like finishing, watermarks, etc.) without installing traditional drivers. Vendors are developing PSAs for Mopria-certified devices.

10. **Mopria:**

    An industry consortium that develops standards for universal, driverless printing and scanning. WPP relies on Mopria-certified printers to ensure basic printing works without a PSA. Learn more at www.mopria.org.

WPP Terms



11. **Fax Printer:**

    Virtual Windows printer used for faxing; automatically removed when WPP is enabled and must be manually reinstalled if needed.

12. **XPS (XML Paper Specification) Printer:**

    Microsoft's digital print-to-file format; removed under WPP.

13. **Secure Printing:**

    A general term for protecting print jobs from interception or tampering; WPP enforces this by limiting driver risk.

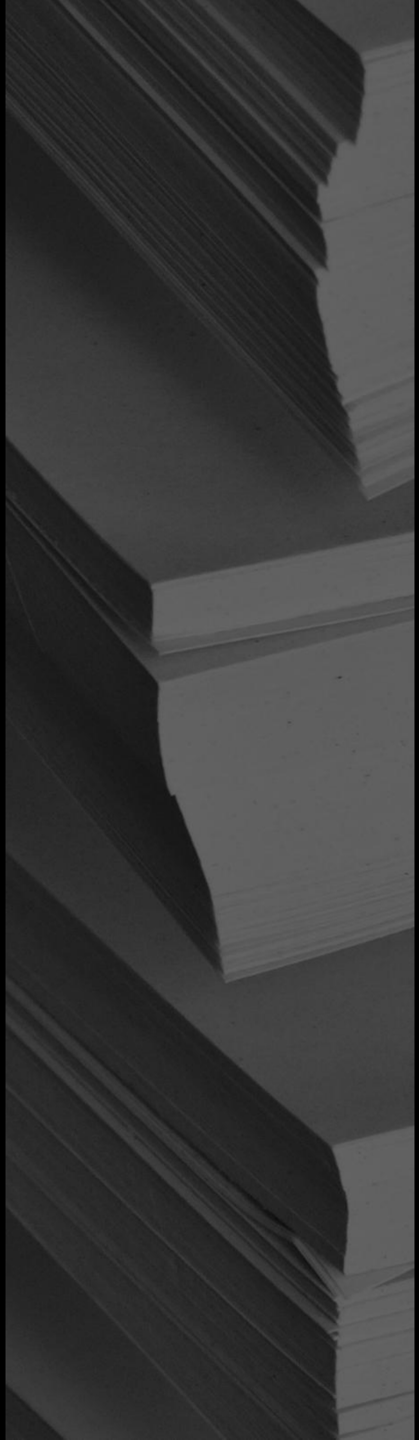
14. **Driverless Printing:**

    Printing without vendor-specific drivers; enabled by WPP through the IPP Class Driver.

15. **Zero Trust Printing:**

    Applying Zero Trust security principles to printing by removing untrusted drivers and enforcing least privilege, as WPP does.

WPP Terms



16. Microsoft Universal Print:

A cloud-based, driverless print management service built into Microsoft 365. It replaces traditional print servers by using point-to-point IPP printing between Windows clients and cloud-registered printers.

17. Entra ID:

Microsoft's modern identity and access management platform for authentication and authorization across Microsoft 365, Azure, and enterprise cloud services.

18. Zero-Day Vulnerability or Attack:

A previously unknown software vulnerability that attackers exploit before a vendor has time to issue a patch—giving defenders "zero days" to prepare. PrintNightmare was a zero-day vulnerability.

Something missing?

Readers of this eBook can provide direct input regarding the report to standards@yourmpsa.org to be considered for future amendments or additional educational formats like live stream events or blog articles presented by the MPSA.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Join the MPSA

https://yourmpsa.org/memberships/

MPSA
MANAGED PRINT
SERVICES ASSOCIATION