Choosing a deployment model: workstation PDAgent, print-server-only or Universal Print

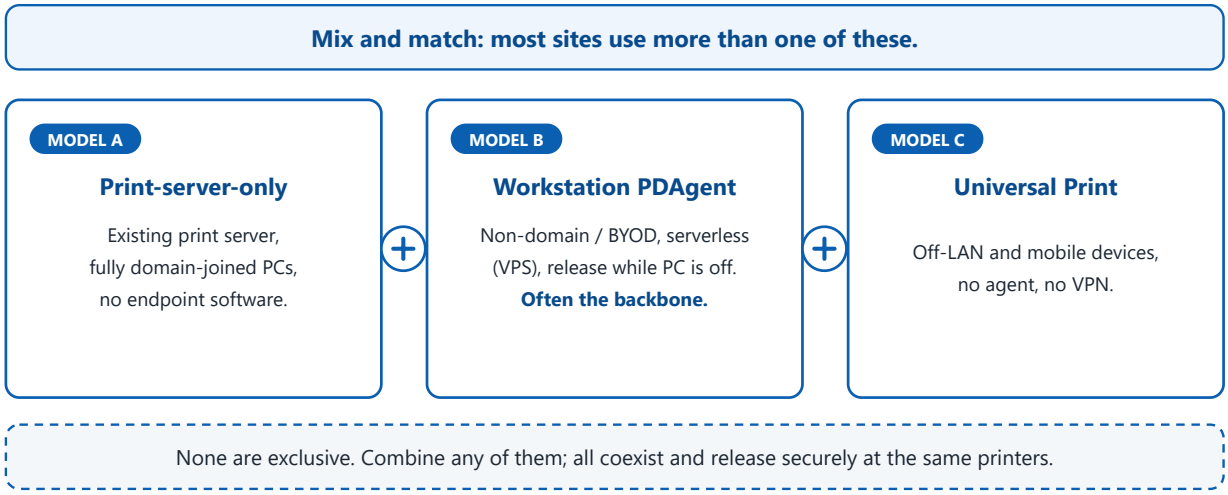
Print Director gives you three supported ways to get Windows print jobs under management. The choice shapes reliability, how users authenticate, whether you need a server on site at all, and whether a user can release a held job when their own PC is switched off:

- **Print-server-only (Model A).** PDAgent is installed only on your existing Windows print server. Client PCs keep printing the way they do today, by connecting to **shared print queues** on that server.
- **Workstation PDAgent (Model B).** PDAgent is installed on every user PC (typically pushed by Group Policy or your endpoint tool). Each PC prints to a local queue that either forwards jobs to a central hold point or holds them on the PC itself, which means it works **with or without a server on site**.
- **Microsoft Universal Print (Model C).** No agent on user devices at all. Users print to a Universal Print share in the cloud, Microsoft's connector pulls the job down to a Print Director-controlled queue on your server, and Print Director holds it there for secure release.

You do not have to pick just one. The three models are not mutually exclusive; they are simply names for ways of capturing print jobs. Most sites combine two or more, for example workstation PDAgent for staff on the LAN plus Universal Print for off-network devices, all releasing securely at the same printers. Match each part of your fleet to the model that suits it, and mix freely.

All three work, and Print Director has supported the first two for years. But the Windows platform has changed underneath the print-server model since 2021, and most new deployments, and a growing number of existing sites, now standardise on **workstation PDAgent** as their backbone. This guide explains why, and helps you pick the right mix for your environment.

Three building blocks (mix and match)



The three models are building blocks, not a one-time choice. Most sites combine two or more, all releasing at the same printers.

The models at a glance

	Print-server-only (Model A)	Workstation PDAgent (Model B)	Universal Print (Model C)
PDAgent installed on	The print server only	Every user PC	The PD server (no agent on user devices)
Client PCs submit via	Shared Windows print queues on the server	A local queue installed by PDAgent	A Universal Print share in the cloud (built into the OS)
Server required on site	Yes	**Optional** (can be VPS-hosted)	Yes (runs the connector)
Desktop footprint	None	PDAgent service (approx. 5 MB), GPO-deployable	None
Depends on Windows print sharing (SMB / spooler RPC)	**Yes**	No	No
Depends on server-side driver delivery (Point and Print)	**Yes**	No	No (no driver on the device)
Works for non-domain / BYOD / off-domain machines	Poorly	**Yes**	**Yes** (Microsoft Entra ID)
Off-network / internet printing without a VPN	No	No	**Yes**
Release a held job while the user's PC is off	Yes	**Yes** (forward-to-hold-point variant)	Yes (held on the server)
Interactive billing / rule pop-ups on the desktop	No	**Yes**	No
Central queue auto-deploy, update and removal	Limited	**Yes**	n/a

Secure release, the rules engine, pricing and billing, and job tracking are **identical in every model**. The difference is entirely in how jobs get from the user's application into Print Director, and how users are identified. Because these are only capture methods, a single site can run any combination of them at once.

Model A: Print-server-only (shared queues)

How it works. You install PDAgent on the Windows print server. The server hosts shared print queues, users connect to them exactly as they always have, and PDAgent captures each job as it arrives at the server, holds it for secure release, applies rules and records it.

What it is good for:

- **Zero desktop footprint.** Nothing is installed on user PCs. For a locked-down, fully domain-joined estate that is already printing happily through a print server, this is the least intrusive option.
- **One place to manage.** Queues, drivers and capture all live on one machine.

What it depends on, and why that is now a risk. This model leans entirely on Windows print sharing, and Microsoft has spent the last few years hardening or removing the exact mechanisms it relies on:

- **Shared-queue connectivity depends on SMB and the spooler's RPC interface.** Since the *PrintNightmare* patches of 2021, and the mandatory SMB signing introduced with Windows 11 24H2 and Windows Server 2025, these paths are progressively locked down. A number of Print Director sites have seen client PCs intermittently fail to reach or install from a shared queue after these updates, and moved to workstation PDAgent to get off the shared-queue path entirely.
- **Driver delivery depends on Point and Print.** Shared queues push the printer driver to the client automatically. Post-PrintNightmare, installing a driver from a server increasingly requires local administrator rights by default, which breaks silent driver delivery to standard users.
- **Identity depends on the Windows domain.** Shared-queue printing assumes the client is domain-joined and authenticating with Kerberos or NTLM. Non-domain PCs, personal laptops and contractor machines are awkward at best.

None of this stops the print-server model working today. But it is swimming against Microsoft's direction of travel (see *Why this matters now* below), and it is the source of most "printing worked before the last Windows update" support calls.

Model B: Workstation PDAgent

How it works. PDAgent runs as a service on each user PC. It installs a **local** print queue, so the user prints to a queue on their own machine rather than to a server share. From there, the job follows one of two paths:

- **Forward to a hold point (recommended for most sites).** The local queue is configured to forward the job to a central PDAgent (typically your server), which **captures and holds it for secure release**. Because the job now lives on the hold point, the user can walk to any printer and release it **even if their own PC is asleep, switched off or has left the building**. This is the behaviour most customers want, and it is configured as a standard queue deployment (see *How to deploy local queues that will send jobs to the server*).

  > **Use IPPS for network transport where supported.** Print Director 2.5.14 supports IPPS forwarding to the server and IPPS delivery to the printer. Configure each network hop to use IPPS to encrypt that hop; upgrading alone does not change existing LPR configurations.

- **Hold on the user's PC (single hop).** The job is captured and held on the user's own PC until they release it, then goes **directly** to the printer in a single hop, never touching a server. This has two real advantages:
  - **It supports serverless environments.** With jobs waiting on each user's PC, you do not need a print server on site at all. The PDServer can be VPS-hosted in the cloud.
  - **It is more secure.** The document is held in one place only, on the user's own PC, and travels a single hop to the printer. That is one fewer copy at rest, and one fewer network hop for anyone to intercept, than forwarding through a server.

  The trade-off is that **the user's PC must be reachable at the moment they release the job.** A PC that has gone to sleep (a laptop or a desktop, depending on its power settings) cannot serve the job until it wakes. In practice this is a matter of setting expectations rather than a hard limit: if a user tries to release while their PC is unreachable, **the printer panel tells them so**, and they simply wake their PC and release again. Many customers run this model successfully with laptops.

> **Held jobs wait on a PDAgent, not "at the printer".** In every variant the document is held by a PDAgent (on the server or on the user's own PC) and is sent to the printer only when the user authenticates and releases it. Nothing is stored on the printer itself while it waits.

What it is good for:

- **Independence from Windows print sharing.** No shared queues, no Point and Print driver push, no reliance on the spooler's RPC surface. The SMB and PrintNightmare hardening described above simply does not apply to the capture path, which is why sites hit by those changes move here.
- **Serverless / VPS-hosted sites**: no on-premises server required, as above.
- **Mixed domain / non-domain fleets**: covered in its own section below, because it is usually the deciding factor.
- **Release without your own PC**: via forward-to-a-hold-point, above.
- **Interactive desktop features.** Billing account pop-ups, rule confirmation and warning dialogs, and user notifications appear in the user's own session, which is only possible with PDAgent present on the workstation.
- **Central queue lifecycle.** Queues can be auto-deployed by PDAgent, hostname pattern, IP range or user login, updated centrally, and removed automatically, without touching each machine by hand.

The cost: PDAgent has to be present on the endpoints. It is a small service (about 5 MB) and is routinely rolled out with Group Policy or any endpoint management tool (see *Group Policy Deployment of PDAgent*), so for most organisations this is a one-time deployment step rather than an ongoing burden.

Local capture: loopback LPR or IPPS

A Windows queue that sends to PDAgent on **127.0.0.1 (loopback)** keeps that capture hop entirely on the same machine. **Loopback LPR is suitable for this purpose:** there is no off-device transport and therefore no plaintext print data crossing the network on that hop.

The benefit of **loopback IPPS** is compatibility with **Windows Protected Print**. Use it when that compatibility is needed. There is no transport-security reason to replace a working loopback LPR configuration, including the local capture used by the Universal Print and Lasernet integrations.

Treat subsequent network hops separately. Local capture over loopback LPR does not prevent using IPPS when forwarding a job to another machine or delivering it to a printer.

Model C: Microsoft Universal Print (no agent on user devices)

How it works. Users print to a **Universal Print share** in the Microsoft cloud, which is built into Windows, macOS, iOS, iPadOS and Android, with **no print driver, queue or VPN on the device**. Microsoft's Universal Print Connector, installed on your Print Director server, pulls each job down into a **Print Director-controlled Windows queue**. Print Director captures it, attributes it to the right person (read from the connector's log), and **holds it on the server for secure release**, then sends it to the printer when the user authenticates and releases.

What it is good for:

- **Off-network printing with no agent and no VPN.** This is the answer when the goal is "users on devices off our LAN must print to our office printers".
- **Entra ID-only users.** Works for users who have only a Microsoft Entra ID account, with no on-premises Active Directory identity.
- **No endpoint footprint.** Nothing to deploy to user devices.

What to keep in mind:

- **It still needs a Print Director server** on site (or VPS) to run the connector and hold jobs, so it is not a serverless model.
- **It requires Print Director 2.5.12.1 or later**, an eligible Microsoft 365 / Universal Print licence, and the connector co-located with the capturing agent.

Universal Print is often deployed **alongside** Model A or B: workstation PDAgent for staff on the LAN, Universal Print for off-network devices, both releasing at the same printers. Full setup is in *How to integrate Microsoft Universal Print with Print Director*.

Why this matters now: the Windows platform is moving away from the print-server model

The print-server model is not deprecated by Print Director. It is being undercut by Microsoft. Four overlapping changes matter:

1. **PrintNightmare hardening (from 2021).** After CVE-2021-34527, Microsoft tightened Point and Print so that installing or updating a printer driver from a server generally needs administrator rights. Silent driver delivery to standard users through a shared queue, the thing that made the print-server model effortless, no longer works the way it did.
2. **Mandatory SMB signing (Windows 11 24H2, Windows Server 2025).** SMB signing is now **required by default**: on Windows 11 version 24H2 for both inbound and outbound connections, and on Windows Server 2025 for outbound connections. This is good security, but it has broken access to file and print resources that cannot negotiate signing, and it has made shared-queue connectivity more fragile in mixed-vintage environments.
3. **The NTLM phase-out.** Microsoft deprecated NTLM in 2024 and is retiring it in phases, with the goal of disabling it by default in a future Windows release in favour of Kerberos. Shared-queue authentication that still leans on NTLM is on borrowed time.

4. **Windows Protected Print and the end of third-party printer drivers.** Windows Protected Print (WPP), introduced with Windows 11 24H2 and Windows Server 2025, removes third-party print drivers and prints only through the built-in **IPP class driver**. In parallel, Microsoft has published an end-of-servicing timeline for the classic v3/v4 drivers that server-hosted queues depend on:

Date	Change
15 January 2026	No new third-party printer drivers published to Windows Update (Windows 11+, Server 2025+).
1 July 2026	Windows prefers the built-in IPP class driver over any installed third-party driver.
1 July 2027	Third-party printer driver updates stop, except for security fixes.

   Microsoft has indicated WPP is intended to become the default in the 2027 timeframe. A print-server model built around a shared, vendor-driver queue is exactly the pattern this transition targets. Print Director 2.5.14 supports the modern IPP-based print path, so the workstation PDAgent model continues to work cleanly as WPP rolls out.

The pattern we see in the field: customers who hit shared-queue reliability problems after a Windows feature update, most commonly after the SMB signing and PrintNightmare changes, resolve them by deploying PDAgent to the workstations and forwarding to a hold point, using IPPS for the network hop where supported. This avoids Windows print sharing. Where Windows Protected Print is enabled, use the supported IPP-based queue configuration.

Mixed domain / non-domain environments: usually the deciding factor

Shared-queue printing assumes every client is domain-joined and authenticates against the domain. That assumption fails for a large and growing share of real fleets: personal laptops, BYOD, remote or hybrid staff, contractors, lab and kiosk machines, and Macs.

Workstation PDAgent authenticates the Print Director user itself, independently of Windows domain membership. It supports several modes so you can match each site:

- **Map the signed-in OS user** to a Print Director user automatically (with optional auto-add), for domain PCs where the OS identity is trustworthy.
- **Prompt for a Print Director login** on the workstation, so a non-domain or shared machine still identifies the correct user. See *How to configure PDAgents for user login*.
- **Self-service registration with email verification.** Where you do not want to pre-create every account, a user can register their own Print Director account from the PDAgent client and confirm it by email. This is ideal for guest, contractor and BYOD scenarios where the person is not in your directory at all. See *PDAgent Client user registration*.

The practical result: **a non-domain PC prints and releases through Print Director without any domain plumbing.** Its queue forwards to the hold point, PDAgent identifies the user independently of the domain, and release works like any other machine. Achieving the same thing through server-hosted shared queues ranges from painful to impossible. (Universal Print is the other domain-independent option, using Microsoft Entra ID identity instead.)

Which models should I use?

You can use more than one, and most sites do. The lists below are not exclusive: match each part of your fleet to whichever models fit, and combine them.

Use workstation PDAgent (Model B) as your backbone if any of these are true:

- You have non-domain, BYOD, remote or contractor machines that need to print.
- You want a serverless / VPS-hosted deployment with no print server on site.
- You have hit, or want to avoid, shared-queue reliability problems after Windows updates (SMB signing, PrintNightmare, driver changes).
- You want billing pop-ups, rule confirmation dialogs, or desktop notifications.
- You want centrally managed queue deployment and driver lifecycle without touching each PC.
- You are planning for Windows Protected Print and the retirement of third-party drivers.

Add Universal Print (Model C), alongside either of the above, if:

- Users need to print to your office printers from off-network devices without a VPN.
- You are an Entra ID / Microsoft 365 organisation with eligible Universal Print licences.
- You want no software deployed to user devices.

Print-server-only (Model A) can be the whole answer if all of these hold:

- The estate is fully domain-joined and centrally managed, with no BYOD or off-domain machines.
- Shared-queue printing is currently reliable and you are not seeing update-related breakage.
- You specifically want no software on endpoints and do not need desktop pop-ups.
- You are comfortable revisiting the decision as Windows Protected Print rolls out.

Many organisations run a **hybrid**: PDAgent on the server or VPS as the central hold-and-release point, PDAgent on workstations forwarding to it, and Universal Print for off-network devices, all releasing at the same printers.

What you keep in every model

Choosing between these models does **not** change the parts of Print Director users and administrators interact with. In all three you keep:

- **Secure release** (release held jobs at the device after authenticating).
- **The rules engine** (force mono, force duplex, quotas, warnings, cancellations).
- **Pricing and billing**, including account selection and quotas.
- **Full transaction tracking and reporting.**
- **Offline operation**, with the local cache database keeping printing working when the central database is unreachable.

Only the capture and authentication path changes.

Related

- *How to install PDAgent*: installing the agent on a server or workstation.
- *Group Policy Deployment of PDAgent*: rolling PDAgent out to every workstation.
- *How to deploy local queues that will send jobs to the server*: the queue deployment that forwards a workstation's jobs to a hold point so they can be released while the user's PC is off.
- *Auto-configure queues to use the PDAgent LPD service*: pointing a local queue at PDAgent.
- *How to configure PDAgents for user login*: prompting users to identify themselves on the workstation.
- *PDAgent Client user registration*: self-service account registration with email verification.
- *How to integrate Microsoft Universal Print with Print Director*: the agentless, off-network model.
- *How to deliver print jobs securely with IPPS*: encrypting the final PDAgent-to-printer hop.

References

Microsoft platform changes referenced above (verify the dates against the source before relying on them, as Microsoft has adjusted this timeline more than once):

- End of Servicing Plan for Third-Party Printer Drivers on Windows: https://learn.microsoft.com/en-us/windows-hardware/drivers/print/end-of-servicing-plan-for-third-party-printer-drivers-on-windows
- SMB security hardening in Windows Server and Windows Client: https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-security-hardening
- Control SMB signing behavior: https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-signing
- Advancing Windows security: disabling NTLM by default: https://techcommunity.microsoft.com/blog/windows-itpro-blog/advancing-windows-security-disabling-ntlm-by-default/4489526

Print Director™ is developed by Blue Swift Software CC.

Print Director version at time of publish: 2.5.15.3. Publish date: 30/10/2026.