Print Director Technical Requirements

Applies to Print Director 2.5.14 and later.

Document Objectives

This document outlines the minimum and recommended hardware and operating system requirements for the Print Director suite of applications. It provides a brief description of each software module and specifies the port usage requirements.

Database Requirements

Print Director supports all versions of Microsoft SQL Server from 2012 to 2025. Express editions are fully supported. Please consult the Microsoft literature for the minimum requirements.

Note the built-in limits of SQL Server Express before choosing it for a production site:

- **10GB maximum database size.** Print Director's transaction history accumulates over time, and busy sites have reached this limit in the field. When the limit is reached, no further transactions can be recorded until history is cleared or the database is moved to a higher edition.
- **4 CPU cores and approximately 1.4GB of buffer pool.** On large fleets (several thousand workstation agents, or heavy secure-release use) these caps become the limiting factor before Print Director does.

SQL Server Standard or higher is recommended for large fleets and for sites with high transaction volumes.

Print Server Requirements

The minimum and recommended requirements listed below are expressed with the assumption that the server will not be running any other services (e.g. domain controller, Exchange, etc). Should the server be running other services, the specifications below should be adjusted accordingly.

Operating System

- PDServer: 64-bit Windows only. Windows 10 (version 1607) and upwards, Windows 11, Windows Server 2012 R2 and upwards. Windows Server 2016 or later is recommended (Server 2012 R2 requires Microsoft Extended Security Updates).
- PDAgent, Resource Manager, PDReports, DBTools: All Windows desktop operating systems from Windows 7 SP1 upwards. All Windows Server operating systems from Server 2012 R2 upwards.
- ARM64 Windows (Windows 11 on ARM, tested): PDAgent and Resource Manager are fully supported, including print queue deployment with driverless configurations and with manufacturer drivers where the manufacturer publishes an ARM64 driver. PDServer is fully supported with one exception: report exports that rely on the Crystal Reports runtime (scheduled report emailing) are not available. PDReports is not supported on ARM64 because the Crystal Reports runtime is not supported on ARM64.

Runtime

- PDServer's core service is a self-contained .NET 10 application: no separate .NET runtime installation is required for it. Its companion service uses .NET Framework 4.8.
- PDAgent, Resource Manager, PDReports and DBTools require .NET Framework 4.8 and above.

Free Hard Drive Space

Installation Files

The Print Director modules installed on a Print Server will use approximately 400MB of hard drive space.

Hard Drive Containing the Held-Job Spool Folder

More importantly, the size of the hard drive hosting the spool folder for Secure Document Release must be correctly allocated. Print Director holds the spool files of jobs waiting for release; until the user releases (or the auto-delete timeout removes) a job, its spool file occupies space on the hard drive.

From version 2.5.14, a print-queue setting determines where each queue's held jobs wait: on the machine running the PDAgent (the print server, or a PC with local print queues), or on the PDServer. Jobs received by Email to Print are also stored at the PDServer. Apply the sizing guidance below to the drive hosting the spool folder on whichever machine holds the jobs; where both modes are in use, apply it to both.

The amount of space required depends on how image intensive the majority of jobs are.

Recommendations for mostly text-based printing:

- 0-5 multi-functional printers (MFPs): 40GB free space
- 5-50 MFPs: 100GB free space
- 50-100 MFPs: 200GB free space

Recommendations for image intensive printing (e.g. advertising industry):

- 0-5 multi-functional printers (MFPs): 200GB free space
- 5-50 MFPs: 500GB free space
- 50-100 MFPs: 1TB free space

RAM

The minimum requirement for RAM is 2GB. The recommended requirements are based on the number of MFPs hosted by the PDServer:

- 0-4 MFPs: 4GB
- 5-20 MFPs: 8GB
- 20-100 MFPs: 12GB

Deployments that hold large numbers of jobs concurrently in Secure Document Release mode should additionally allow approximately 2GB of RAM per 50,000 concurrently held jobs on the PDServer.

CPU

The minimum required CPU speed is 1.5Ghz single core. Recommended:

- 0-10 MFPs: 2Ghz dual core
- 10-40 MFPs: 2.6Ghz dual core
- 40-100 MFPs: 2.6Ghz quad core

Large Fleets (Workstation Agent Deployments)

Deployments that install the PDAgent on individual workstations (rather than only on print servers) can reach fleet sizes far beyond the MFP counts above. Print Director 2.5.13 has been load-verified at 10,000 concurrently connected PDAgents, each re-registering 10 held jobs on reconnect (100,000 held-job registrations in one startup burst), on a single PDServer with 4 CPU cores and 16GB RAM and with SQL Server running on the same machine. A staggered fleet reconnect of that size completes with server CPU below 10%.

For fleets of this scale, follow the RAM allowance for concurrently held jobs above, and use SQL Server Standard or higher per the Database Requirements section.

Email-to-Print sender identity requirements

Before enabling user matching, the mail administrator must ensure that only senders authorised to use the complete From address can deliver messages to the Email-to-Print mailbox and its aliases. This applies to POP3, IMAP and Microsoft Graph receive accounts.

Print Director selects the print-job owner by matching the message's From address against the configured login-name, primary-email or secondary-email strategies. It does not validate SPF, DKIM, DMARC or Authentication-Results headers. If a forged From address matches a user, the job is attributed to that user and, if printed, uses their account and quota under the normal print rules. Secure release still applies, but does not establish who submitted the email.

Mail-system controls required for user matching

- Restrict mailbox delivery to authenticated, authorised senders. Enforce permission to use the complete From address, including aliases and delegated send-as permissions. Blocking external mail alone is insufficient if an internal sender or relay can submit as another user.
- Cover every mailbox alias and delivery route, including connectors, relays, forwarding and applications that can write to the inbox. A sender-domain allowlist alone does not establish the sender's identity. Protect mailbox credentials and use encrypted connections; these protect mailbox access, not the original sender's identity.
- If external senders are accepted, enforce the receiving gateway's SPF/DKIM/DMARC and anti-spoofing policy, together with controls establishing permission to use the individual From address. Reject or quarantine messages that lack the required assurance before they enter the inbox Print Director polls. Do not rely on a header being present or on the sender's published DMARC policy causing rejection. Internal mail without DMARC needs an equivalent verified submission policy.
- Keep the user email and login mappings accurate and unambiguous. If the mail system cannot provide the required sender assurance, do not enable individual-user matching for that mailbox.

A DMARC pass validates domain use, not the individual mailbox name. Authentication-Results is trustworthy only when the receiving mail system controls its origin and removes forged assertions at ingress. Print Director does not make these checks. See DMARC scope and Authentication-Results trust requirements.

Public or unverified submissions

Use a separate guest-only Email-to-Print configuration for mail whose sender cannot be verified. Set the first user-match strategy to **Do not match**, then choose **Allow guest printing (one-time-PIN for release)** and a dedicated guest user with appropriate limits. Setting the first strategy to Do not match bypasses all user matching. Ensure no other configuration with user matching enabled consumes the same public ingress.

Merely allowing unmatched guests does not protect existing users: an address that matches a user takes the matched-user path first. Guest jobs are recorded against the configured guest user. The emailed PIN controls guest-job release; it does not authenticate the original From address or prevent unsolicited jobs from consuming storage. Disable receipt if neither verified-user nor guest printing is intended.

Verify before enabling receipt

Use test accounts and a harmless attachment. Confirm that a legitimate authorised sender is assigned to the intended Print Director user. Then verify that external mail forging that user's From address, an internal sender without send-as permission, and mail carrying a forged Authentication-Results pass cannot enter the matched-user inbox. Check every permitted delivery route and confirm rejection or quarantine in the mail-system logs.

For guest-only receipt, verify that even a From address matching an existing user produces a guest job, with release requiring its guest PIN. Record the mail administrator responsible for these controls and repeat the checks after changes to connectors, forwarding, aliases or mail-security policies.

Module Description

PDServer

Self-contained .NET 10 Windows service with a .NET Framework 4.8 companion service (64-bit Windows 10 / Server 2012 R2 and above; Server 2016 or later recommended)

- Can be installed on a single server or multiple servers (multiple servers to prevent MFP authentication requests from traversing unreliable WAN links).
- Performs communication with the embedded applications on the MFPs (Authentication and PullPrint), served over HTTPS.
- Hosts the browser-based administration pages and REST API on its HTTPS port.
- Can store held jobs for print queues configured to hold jobs at the server, and for Email to Print.
- Executes scheduled tasks (e.g. report emailing and directory synchronisation, including Microsoft Entra ID).
- Does not necessarily have to be installed on the print server.
- PDAgents connect to PDServer(s) over a single outbound HTTPS connection (persistent, real-time).
- Can operate in offline mode (i.e. if the SQL Server connection is lost it caches transactions to a local DB).

PDAgent

.Net Framework 4.8 windows service (supports Windows 7 SP1 and above, Server 2012 R2 and above)

- Monitors the print queues for the MFPs and printers.
- Holds jobs sent to local print queues (unless the queue is configured to hold its jobs at the PDServer).
- Waits for communication from PDServer before releasing the jobs (i.e. user logs in and selects the jobs to be released).
- Receives jobs via the IPP/IPPS and LPR protocols. IPP is the default protocol for the print queues Print Director deploys on Windows, which enables support for Windows Protected Print; IPP is also used by AirPrint on Apple devices and Mopria on Android devices.
- Required to be installed on the print server(s) or client PCs with local print queues or print-popup requirements.
- Connects to the SQL Server via .Net.
- Connects to PDServer(s) via a single outbound HTTPS connection.
- Can operate in offline mode (i.e. if the SQL Server connection is lost it caches transactions to a local DB).

Resource Manager

.Net Framework Windows forms application (supports Windows 7 SP1 and above, Server 2012 R2 and above)

- Configuration module for Print Director.
- Used to maintain user settings (PIN numbers, email address, popup behaviours, etc).
- Used to configure printer settings (pricing, rules, etc).
- Used to install the embedded applications to the MFPs.
- Can be installed on any number of workstations and connected to the database.

PD Reports

.Net Framework Windows forms application (supports Windows 7 SP1 and above, Server 2012 R2 and above)

- Reporting module for Print Director.
- Can be installed on any number of workstations and connected to the database.
- Not supported on ARM64 Windows (the Crystal Reports runtime does not support ARM64).

DBTools

.Net Framework Windows forms application (supports Windows 7 SP1 and above, Server 2012 R2 and above)

- Creation of the Print Director database.
- Backup and restore of the database.
- Can be installed on any number of workstations and connected to the database.

Port Usage

The PDAgent and PDServer will make exceptions in Windows Firewall automatically. For other firewalls, please see the port requirements below. All ports are configurable; the values listed are the defaults for new installations. Versions prior to 2.5.14 used different defaults for the PDServer web services (58113/58114); those ports are no longer used.

PDServer

- Listens on TCP port 48116 (HTTPS): the primary port. Carries the administration web pages, the REST API, PDAgent communication, Resource Manager communication, and the embedded MFP applications (Konica Minolta, Lexmark, HP).
- Listens on TCP port 48117 (HTTP): optional non-TLS port.
- Listens on TCP port 48002 (TLS): Konica Minolta OpenAPI/SDK communication with embedded KM MFPs.
- Listens on TCP port 20115: legacy Lexmark embedded application (PDLexmark2 fleets only; PDLexmark3 and above use the HTTPS port above).
- Listens on TCP port 5114: keypad attached MFPs.

PDAgent

- Listens on TCP port 631 (IPP) and TCP port 9633 (IPPS, TLS) to receive print jobs via the IPP protocol: the default protocol for Print Director deployed Windows print queues (enabling Windows Protected Print support), and also used by AirPrint on Apple devices and Mopria on Android devices.
- Listens on TCP port 515 to receive print jobs from print queues using the LPR protocol.
- Listens on TCP port 20113 for legacy communication from other Print Director modules.
- Requires no inbound port for PDServer communication: the agent makes a single outbound HTTPS connection to the PDServer on port 48116.

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