



Release Notes for RICOH InfoPrint Manager™ for Windows 4.15.2

Release Notes for RICOH InfoPrint Manager for Windows 4.15.2

Copyright © 2000-2026 Ricoh Company Ltd. All rights reserved.

This edition applies to InfoPrint Manager for Windows Version 4 Release 15.2. It is available in the RICOH Software Information Center at <https://help.ricohsoftware.com/swinfocenter>.

We are moving our InfoPrint Manager forum discussions to the new **Community** platform at <https://support.ricohsoftware.com> for a more streamlined, user-friendly experience. Register your account and start participating in the InfoPrint Manager forum threads by clicking the **Community** button at the top of the webpage. All previous posts have been successfully transferred, so no discussions have been lost.

An online platform for InfoPrint Manager customers to engage the support team is also available at <https://support.ricohsoftware.com>. This platform allows customers to open and manage support tickets across their organization. For more information about registering and working with support tickets using the online platform, go to [https://help.ricohsoftware.com/swinfocenter/ricoh-software-support/support_project.ditamap/\\$/support_using_support_site](https://help.ricohsoftware.com/swinfocenter/ricoh-software-support/support_project.ditamap/$/support_using_support_site).

↓ Note

- To find out if your country supports opening and managing support tickets directly by customers, contact your local Ricoh representative.

InfoPrint Manager provides an Ideas portal for InfoPrint Manager users to submit feedback to the product management team directly from the product interface. The Ideas portal link is <https://ipm-ideas.ricohsoftware.com/>.

All InfoPrint Manager servers and clients must be upgraded to the same version. Do not forget to upgrade any secondary InfoPrint Manager servers.

If you are upgrading multiple servers, keep all clients at the older (4.9.1 or earlier) level until all servers are upgraded to 4.9.2 or later. Then upgrade the clients.

You must agree to the terms of the [Software Maintenance Agreement \(SWMA\)](#) before installing the InfoPrint Manager software.

What's new in Release 4.15.2?

- **Expanded IPP Gateway support for mobile printing**

The IPP Gateway now accepts PWG Raster (`image/pwg-raster`) input and automatically converts it to PDF before submitting jobs to InfoPrint Manager, enabling printing from a wider range of mobile applications and modern IPP clients.

For more information, see *RICOH InfoPrint Manager for Windows: Getting Started*, the “IPP Gateway printer” section.

- **Print Rules now support setting the `font-resolution` attribute**

You can now create Print Rules that use the `font-resolution` attribute on jobs when adding a condition or an action.

For more information, see *RICOH InfoPrint Manager for Windows: Procedures*, the “Configuring print rules” section, or the InfoPrint Manager Web Administration Interface (Web GUI) Help.

- **Added the Delegate Print feature to InfoPrint Select for Linux and macOS**

InfoPrint Select now supports print delegation on Linux and macOS, letting a user authorize another user to release their print jobs on their behalf.

For more information, see *RICOH InfoPrint Manager for Windows: Getting Started*, the “Using InfoPrint Select for Linux ” or the “Using InfoPrint Select for macOS” section, the InfoPrint Select for Linux Help, or the InfoPrint Select for macOS Help.

- **Publications:**

- **English**

- ◆ *RICOH InfoPrint Manager for Windows: Planning Guide*, G550-1071
- ◆ *RICOH InfoPrint Manager for Windows: Getting Started*, G550-1072
- ◆ *RICOH InfoPrint Manager for Windows: Procedures*, G550-1073
- ◆ *RICOH InfoPrint Manager: High Availability Guidelines*, G550-20261
- ◆ *RICOH InfoPrint Manager: Reference*, S550-1052
- ◆ *RICOH InfoPrint Manager: PSF, Server, and Transform Messages*, G550-1053
- ◆ *RICOH InfoPrint Manager: Secure Print: Installing and Configuring*, G550-20129
- ◆ *RICOH InfoPrint Manager: SAP Planning and Configuring Guide*, S550-1051
- ◆ *AFP Conversion and Indexing Facility: User's Guide*, G550-1342
- ◆ *RICOH InfoPrint Manager: Dictionary of Keywords*, S550-1188
- ◆ *RICOH InfoPrint Manager AFP2PDF Transform Feature: Installing and Using*, G550-1057
- ◆ *Page Printer Formatting Aid for Windows: User's Guide and Reference*, S550-0801
- ◆ *RICOH InfoPrint Manager: Installing InfoPrint Manager Transform Feature*, G550-20160

- **Japanese**

- ◆ *RICOH InfoPrint Manager for Windows: Planning Guide*, G550-20267
- ◆ *RICOH InfoPrint Manager for Windows: Getting Started*, GB88-4106
- ◆ *RICOH InfoPrint Manager for Windows: Procedures*, GB88-4108

Limitations

Accounting information when printing PDL nested jobs to Ricoh controller devices reports 0 (zero) pages completed

Accounting information when printing PDL nested jobs to Ricoh controller devices reports 0 (zero) pages completed when InfoPrint Manager is configured to report job completed when printed (wait-for-job-completion is enabled) and when using InfoPrint TCP/IP Network Port Monitor. If you encounter this problem, contact your local Ricoh printer representative.

Single Cell Halftone

The small (one bit monochrome) images that are transformed with transparency enabled are not transformed with the Single Cell algorithms. The native PostScript® data streams that use the imagemask operator are transformed using the original halftone algorithms. The PDF data

streams that process small (one bit monochrome) images with transparency enabled also use the original algorithms.

Make sure that all x64 kernel-mode software is signed

Previous x64 versions of Microsoft® Windows Server® did not require drivers to be signed. However, in the x64 version of Windows Server, all kernel-mode software (including drivers) that runs on the computer must have a signature.

Indexed Multiple Data Sets

MVS™ Download Receiver cannot be used with multiple data sets that have already been indexed (contain AFP TLEs).

InfoPrint Manager for Windows and RICOH ProcessDirector™ for Windows limitation

InfoPrint Manager for Windows and RICOH ProcessDirector™ for Windows cannot coexist on the same Windows machine.

Interchanging set version attribute

The sap2afp transform command does not create IS/3 compliant AFP output when converting an ABAP® file by specifying 3 as a value for the **-is** flag. The sap2afp transform command creates IS/3 compliant AFP output only when the input file is an OTF file.

Capitalization of object names

InfoPrint Manager object names are case-sensitive. However, Windows API is not case-sensitive. Because of this limitation, you cannot have two objects with the same name, even if one of the names has uppercase letters.

When you use Microsoft V4 printer drivers, all InfoPrint Manager port monitors (InfoPrint Select, InfoPrint TCP/IP Port Monitor, InfoPrint Port Monitor) are not supported

Use V3 print drivers either shipped with the Windows installation base or downloaded from the manufacturer's website.

InfoPrint Transform Manager feature limitations

- InfoPrint Manager for Windows and InfoPrint Transform Manager feature for Windows cannot coexist on the same Windows machine.
- SAP2AFP transformer does not support SAP® ABAP document format.

Job Viewer limitations

- When viewing an AFP Job that uses a form-definition with an n-up value set, the n-up value will be ignored.
- Embedded PDF files can be viewed only when the job is viewed page by page. When viewing the full document, the embedded PDF files are not supported.

Known problems and workarounds

Longer processing for color text that uses embedded fonts

When transforming PDF with color text that uses embedded font subsets to black and white or color AFP output, the rip processing can take longer. If you use **savevm=false**, this performance will improve. However, we recommend using the current default of **savevm=true** because, in some cases, PDF input files with many embedded font subsets might fail to transform. The **savevm** option appears on the **ps2afp/pdf2afp** command line as: **-pragma pdf2psoptions=savevm=true**.

Upgrading SAP Clients on Linux

If you are upgrading your SAP clients, update the LOMS definitions for all your InfoPrint Manager printers to point to the updated **ipm_submit**, **ipm_dev_query**, **ipm_job_query**, and **ipm_job_cancel** commands by removing all trailing **.linux** options from the OMS commands. For more information on modifying the OMS commands, see *RICOH InfoPrint Manager: SAP Planning and Configuring Guide*.

License clock tampering problem

If InfoPrint Manager is installed on a machine with the system date and time older than the current date, InfoPrint Manager server starts issuing the error: "5010-901 InfoPrint Manager detected a time tampering problem".

Contact your support personnel and ask them to make sure that the system time is synchronized with the Internet time server. Remove the license that caused the problem and reinstall it.

Job status and device timeout setting

The device timeout setting can cause the jobs to be reported as failed and the actual destination state to be changed to **needs key operator** when InfoPrint Manager is configured to provide accurate job status (by enabling the **wait-for-job-completion** attribute), which requires the backend program to wait for the jobs to print completely.

If your physical printer has a timeout setting, make sure it is disabled or the timeout value is higher than the necessary time to print your largest possible job when you enable the **wait-for-job-completion** attribute. For Ricoh printers, you can use Remote Maintenance by telnet to make the necessary changes to the direct printing port settings (**diprint** command).

AFP with inline resources might misprint in multi-document jobs via pdpr command or Web GUI

AFP documents that contain inline resources, as well as ZIP files containing AFP documents with inline resources, might be misprinted when submitted as multiple documents in a single job. To avoid this issue, submit each file separately.

Unsupported operators in Print Rules configuration on Web GUI

When configuring Print Rules in Web GUI, users cannot apply the logical operators **Is Greater Than** ("**>**") and **Is Less Than** ("**<**") for attribute value comparisons. The **Is Greater Than or Equals** ("**>=**") and **Is Less Than or Equals** ("**<=**") operators should be used instead.

The operators **Has a value (set)** and **Has no value (not set)** are likewise unsupported. As a workaround, these operators can be managed from the command line.

Security fixes included in Release 4.15.2

Release **4.15.2** includes fixes for these CVEs:

Apache® Tomcat® 10.1.57	EncryptInterceptor uses CBC mode - vulnerable to padding oracle attack CVE-2026-29146
	OCSP soft-fail bypass in CLIENT_CERT auth CVE-2026-29145
	SNI/hostname case mismatch bypasses strict SNI checks CVE-2026-32990
	Request smuggling via unvalidated HTTP/1.1 chunk extension CVE-2026-24880
	Open redirect via LoadBalancerDrainingValve when node is draining CVE-2026-25854
	TLS cipher preference order not preserved when TLS 1.3 suites added CVE-2026-29129
	 Incomplete fix for CVE-2026-29146 — EncryptInterceptor fully bypassable CVE-2026-34486
	OCSP soft-fail bypass on FFM connector in CLIENT_CERT auth CVE-2026-34500
	Arbitrary JSON injection in access log via incomplete escaping CVE-2026-34483
	Kubernetes bearer token exposed in log messages CVE-2026-34487
	DIGEST auth allows any unknown user to authenticate with password "null"

	CVE-2026-43512
	Security constraints not applied when multiple constraints share an extension pattern CVE-2026-43515
	Unbounded request body in WebDAV LOCK/PROPFIND (unauthenticated) CVE-2026-41284
	HTTP/2 request headers not validated CVE-2026-41293
	WebSocket client forwards auth header to redirect target CVE-2026-42498
	LockOutRealm case-sensitivity weakens brute-force protection CVE-2026-43513
	AJP secret compared in non-constant time (timing attack) CVE-2026-43514
	Security constraints on default servlet ignore HTTP method restrictions CVE-2026-55956
	XSS via wildcard property mapping in example app CVE-2026-50229
	RewriteValve ornext logic skips conditions incorrectly CVE-2026-53404
	Invalid CRL config silently ignored on FFM connector CVE-2026-53434
	Logged effective web.xml missing special roles and empty auth constraints CVE-2026-55276

	EncryptInterceptor not protected against replay attacks CVE-2026-55955
	EncryptInterceptor secure-configuration requirements not clearly documented CVE-2026-59084
	Incorrect URL decoding in RewriteValve may allow security control bypass CVE-2026-59083
OpenSSL® 3.5.7	Heap use-after-free in PKCS7_verify() CVE-2026-45447
	CMS AuthEnvelopedData may accept forged messages CVE-2026-34182
	Unbounded memory growth in QUIC PATH_CHALLENGE handler CVE-2026-34183
	NULL pointer dereference in QUIC server initial packet handling CVE-2026-42764
	AES-OCB IV ignored on EVP_Cipher() path CVE-2026-45445
	Heap buffer over-read in ASN.1 content parsing CVE-2026-34180
	PKCS#12 / PBMAC1 accepts short HMAC keys CVE-2026-34181
	NULL dereference in password-based CMS decryption CVE-2026-42766
	NULL dereference in CRMF EncryptedValue decryption

	CVE-2026-42767
	Bleichenbacher oracle in CMS_decrypt() / PKCS7_decrypt() (multi-RecipientInfo) CVE-2026-42768
	Trust-anchor substitution via typo in CMP rootCaKeyUpdate CVE-2026-42769
	FFC-DH peer validation uses attacker-supplied q CVE-2026-42770
	Incorrect tag processing for empty messages in AES-GCM-SIV/AES-SIV CVE-2026-45446
	Heap buffer overflow in ASN.1 multibyte string conversion CVE-2026-7383
	Out-of-bounds read in CMS password-based decryption CVE-2026-9076
IBM® Semeru Runtime® Open Edition for Java® – OpenJ9 0.59.0	Pre-auth remote DoS — unauthenticated attacker crashes JITServer with a crafted 32-byte TCP message; PoC available, automatable CVE-2026-6918
IBM Semeru Runtime Open Edition for Java – OpenJDK® 21.0.11	XXE/information disclosure — unauthenticated remote attacker can read critical data; easily exploitable CVE-2026-22016
	Unauthenticated remote DoS — infinite loop/hang; no complexity, no interaction required CVE-2026-34282
	Difficult to exploit; attacker can gain unauthorized access to critical data; requires user interaction CVE-2026-22013

	Uncontrolled resource consumption — remote partial DoS over HTTPS; low complexity CVE-2026-22021
	Integer overflow → out-of-bounds read in OpenType variable font parsing; requires local user interaction CVE-2026-23865
	Remote partial DoS — resource exhaustion in ZIP parsing; difficult to exploit CVE-2026-22018
	Local attacker can read a subset of data; high complexity, local access required CVE-2026-22007
	Local attacker can read a subset of data; high complexity, local access required CVE-2026-34268

CCRs included in Release 4.15.2

Release **4.15.2** includes resolution for these CCRs:

IPM3-1478	Web GUI job properties does not display properly because of the huge number of forms attribute values
IPM3-1489	Change hardcoded default value of pdf2afp transform for agspdl_max_memory parameter from 6000 to 2097151

Trademarks

RICOH InfoPrint Manager™ and RICOH ProcessDirector™ are trademarks of Ricoh Company, Ltd. in the United States, other countries, or both.

These terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

- AIX®
- IBM®
- MVS™
- Semeru Runtime®

Adobe®, Adobe® PDF, and PostScript® are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AlmaLinux OS™ is a trademark of AlmaLinux OS Foundation.

Apache® and Tomcat® are registered trademarks of the Apache Software Foundation in the United States and/or other countries.

Keycloak™ is a trademark of The Linux Foundation® in the United States and/or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

CUPS™ and macOS® are trademarks or registered trademarks of Apple, Inc. in the United States, other countries, or both.

Microsoft®, Windows®, and Windows Server® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java® and OpenJDK® are registered trademarks of Oracle and/or its affiliates.

OpenSSL® is a registered trademark owned by the OpenSSL Software Foundation.

Red Hat®, RHEL®, and Red Hat Enterprise Linux® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Rocky Linux® is the registered trademark of the Rocky Enterprise Software Foundation in the U.S. and other countries.

SAP® and ABAP® are the registered trademarks of SAP SE or its affiliates in Germany and in several other countries.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.