Release Notes for RICOH InfoPrint Manager™ for AIX 4.15.3

Release Notes for RICOH InfoPrint Manager for AIX 4.15.3

Copyright © 1997-2026 Ricoh Company Ltd. All rights reserved.

This edition applies to InfoPrint Manager for AIX Version 4 Release 15.3. 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.

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 4.15.3?

InfoPrint Manager for AIX 4.15.3 is a service release. Details about the updates below will be included in the publications for the next release, InfoPrint Manager for Linux 4.16.0:

- **Added an *Always prompt for login* option to Federated Authentication settings**
  The InfoPrint Manager Web Administration Interface now includes an *Always prompt for login* option in the Federated Authentication settings, available for all supported identity providers (AD FS, PingFederate/CAIA, Okta®, and Keycloak™).
- **Publications:**
  - **English**
    - *RICOH InfoPrint Manager for AIX: Planning Guide*, G550-1060
    - *RICOH InfoPrint Manager for AIX: Getting Started*, G550-1061

- *RICOH InfoPrint Manager for AIX: Procedures*, G550-1066
- *RICOH InfoPrint Manager for AIX and Linux: Configuring and Tuning Guide*, S550-1062
- *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 AIX: Planning Guide*, GB88-4103
- *RICOH InfoPrint Manager for AIX: Getting Started*, GB88–4107
- *RICOH InfoPrint Manager for AIX: Procedures*, GB88–4109

Limitations

Single Cell Halftone

Single Cell Halftone support has a limitation with the provided transparency support. 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.

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 AIX and RICOH ProcessDirector™ for AIX limitation

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

IBM AIX native printing system does not support IPv6.

IBM® AIX native printing system does not support IPv6 , so functions such as: LPD or remote queue, are not be supported.

InfoPrint Transform Manager feature limitations

- SAP2AFP transformer does not support SAP® ABAP document format.

InfoPrint Manager printing limitation on InfoPrint 5000

You cannot print via a hot folder to an InfoPrint 5000 from InfoPrint Manager for AIX version 7.2.

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`.

InfoPrint Manager setup installation

Using the InfoPrint Manager setup graphical installer can cause issues when installing the product. This occurs when the register path is selected and you use the **Back** button after the installer asks for the license key. To avoid this, either have the product license key prepared before the installation process is started or install the product in trial mode and register it after the installation is complete using the License Key Management Application. For more information, see *RICOH InfoPrint Manager for AIX: Getting Started*, G550-1061.

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 accounting for nested PJL jobs

Accounting information reports 0 (zero) pages completed when InfoPrint Manager prints nested PJL jobs to Ricoh controller devices and InfoPrint Manager is configured to wait for the job to print completely (wait-for-job-completion is enabled).

To avoid this situation, use the InfoPrint Manager provided **pioinfo** backend and enable the PJL JOB counting function using the **-w** option with the printer command, for example: `/usr/lib/lpd/pio/pioinfo://ricohdevice.yourcompany.com -w`.

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 4.15.3

Release **4.15.3** includes fixes for these CVEs:

Apache® Tomcat® 10.1.57 → 10.1.61	**DoS via allocation leak in HTTP/2 backlog tracking when a stream is reset** CVE-2026-68763
	Principal lookup could fail open in some cases CVE-2026-68569
	RewriteValve [N] restarts at the second rule and may bypass access control CVE-2026-65927
	Security constraint bypass CVE-2026-65182
	Regression in fix for CVE-2026-41293 can trigger request header mix-up CVE-2026-86350
	AJP DoS via missing request body CVE-2026-78383
	DoS via busy wait during WebSocket close CVE-2026-77791
	Bypass of security constraints for WebSocket endpoints CVE-2026-76183
	HTTP/2 no-authority bypass of strict SNI validation CVE-2026-65637
	Incomplete fix for CVE-2026-34500 — OCSP checks sometimes soft-fail with FFM CVE-2026-86248
	WebSocket DoS due to lost asynchronous write timeout CVE-2026-79677
	OpenSSL/OpenSSL-FFM TLS implementations ignore CRLs when cert uses a keystore CVE-2026-73581

	Authenticated WebSocket session survives end of HTTP session CVE-2026-73180
	Redirect after FORM authentication may bypass method-specific constraints CVE-2026-68525
	Servlet role references can bypass declarative role constraints CVE-2026-66422
	DoS in WebSocket chat example CVE-2026-66299
	Limited replay attack possible with DIGEST authentication CVE-2026-65905
	TOCTOU when setting permissions for Unix Domain Sockets CVE-2026-65183
	WebSocket message smuggling with per-message-deflate CVE-2026-87022
	HTTP/2 DoS via malformed request CVE-2026-78437
	Stale HPACK emitter injects trailers into recycled pooled Request CVE-2026-77762
	Transfer-Encoding honored for HTTP/1.0 requests CVE-2026-77756
	Cross-context authentication mix-up with Jakarta Authentication configured CVE-2026-75973
	HTTP/2 request/response mix-up after error during async processing CVE-2026-101356
	JNDIRealm bind credential validation fails open for non-GSSAPI SASL mechanisms

	CVE-2026-101296
	Possible TLS 1.3 connection failures CVE-2026-93446
	HTTP/2 trailer header cross-contamination CVE-2026-88041
	Jasper JSTL <c:redirect> plug-in implementation omits page abort (SKIP_PAGE) CVE-2026-74049
	OpenSSL-FFM FIPS failure does not prevent start-up CVE-2026-74048
OpenSSL® 3.5.7 → 3.5.9	**DTLS retransmits handshake messages from a stale buffer offset** CVE-2026-84782
	QUIC server double-free processing INITIAL packet CVE-2026-18798
	Heap buffer overflow in CMS AES-WRAP-PAD key unwrapping CVE-2026-63072
	Invalid pointer deref in CMP server via crafted protectionAlg CVE-2026-63076
	Double-free checking OCSP stapled response CVE-2026-35188
	AEAD forgeries with empty ciphertext in EVP_Cipher() CVE-2026-75803
	NULL deref in RPK server signature-algorithm selection CVE-2026-14457
	Excessive memory buffering DTLS records for a future epoch CVE-2026-54874
	Untrusted CMP sender DN used as format string CVE-2026-63073

	CMP indefinite cache growth of ExtraCerts CVE-2026-63074
	QUIC ACK-only packet retention can cause memory exhaustion CVE-2026-63075
	Unbounded memory growth in QUIC server incoming channel queue CVE-2026-14456
	Excessive memory allocation in relative CRLDP processing CVE-2026-35189
	Timing side-channel in scalar multiplication for non-NIST EC curves CVE-2026-54872
	Timing side-channel in SM2 signature generation CVE-2026-77696
IBM® Semeru Runtime® Open Edition for Java® – OpenJ9 0.59.0 → 0.63.0	Recompiled-abstract superclass method incorrectly delegates to interface default method CVE-2026-16441
	-Xtrace method-argument tracing causes buffer underflow CVE-2026-16439
	SIMD arraycmp for Z/P doesn't check for zero-length comparison (Eclipse OMR, bundled with OpenJ9) CVE-2026-16243
	Deeply-nested annotations in a crafted .class file cause a SIGSEGV CVE-2026-16440
	JITServer: malformed messages cause out-of-bounds heap reads and crash (remote DoS) CVE-2026-110938
	JITServer: integer overflow in length handling on connect; pre-auth remote DoS CVE-2026-111074

	JITServer: missing validation of message size and offset fields; crafted payload causes remote DoS CVE-2026-111075
	jdmpview/DTFJ: opening a supplied dump bundle can read a local file and send it to a remote host CVE-2026-97400
IBM Semeru Runtime Open Edition for Java – OpenJDK® 21.0.11 → 21.0.13	Little CMS (lcms2): integer overflow in CubeSize (cmslut.c), overflow check done after the multiplication CVE-2026-41254
	Libraries component vulnerability — unauthenticated remote attacker can modify data via APIs CVE-2026-47063
	Security component vulnerability — unauthenticated remote attacker can read and modify limited data via multiple protocols CVE-2026-60147
	JSSE component vulnerability — unauthenticated attacker via TLS can modify data CVE-2026-46968
	Libraries component vulnerability — unauthenticated remote attacker can cause partial denial of service via APIs CVE-2026-47027
	2D component vulnerability — unauthenticated remote attacker can cause partial denial of service CVE-2026-47021
	JSSE component vulnerability — unauthenticated attacker via TLS can cause partial denial of service CVE-2026-46917
	2D component vulnerability — partial denial of service CVE-2026-47059
	ImageIO component vulnerability — limited unauthorized data modification CVE-2026-47010

	JSSE (TLS) component vulnerability — remote unauthenticated; read and modify all accessible data CVE-2026-114820
	JSSE (TLS) component vulnerability — remote unauthenticated; read and modify all accessible data CVE-2026-91403
	2D component vulnerability — remote; hang or repeatable crash (complete DoS) plus limited data impact CVE-2026-91415
	Libraries component vulnerability — remote unauthenticated; modify some data and read a subset CVE-2026-101516
	Security component vulnerability — remote; create/delete/modify critical data CVE-2026-83374
	JAAS component vulnerability — remote unauthenticated; read a subset of data CVE-2026-83380
	Security component vulnerability — remote; modify some data and read a subset CVE-2026-83381
	JDBC component vulnerability — remote; read all accessible data CVE-2026-83387
	Networking component vulnerability — remote unauthenticated; modify some data and limited availability impact CVE-2026-83395
	JAXP (XML) component vulnerability — remote unauthenticated; partial DoS CVE-2026-83400
	JAXP (XML) component vulnerability — remote; read all accessible data CVE-2026-87290

	Networking component vulnerability — remote unauthenticated; read a subset of data CVE-2026-87291
	Security component vulnerability — remote unauthenticated; modify some data and read a subset CVE-2026-87294
	Networking component vulnerability — remote unauthenticated; modify some data CVE-2026-91332
	JSSE (TLS) component vulnerability — remote unauthenticated; partial DoS CVE-2026-91373
	Libraries component vulnerability — local; needs user interaction; unauthorized data modification CVE-2026-91375
	JDK tools component vulnerability — local; needs user interaction; unauthorized data modification CVE-2026-91379
	Utility component vulnerability — local; modify some data and read a subset CVE-2026-91380
	2D component vulnerability — remote; modify critical data with limited availability impact CVE-2026-91382
	Networking component vulnerability — remote; read all accessible data CVE-2026-91394
	Libraries component vulnerability — remote unauthenticated; partial DoS CVE-2026-91410
	ImageIO component vulnerability — remote unauthenticated; partial DoS CVE-2026-91418

	Networking component vulnerability — remote unauthenticated; modify some data CVE-2026-91451
	Networking component vulnerability — remote unauthenticated; modify some data CVE-2026-91452
	Lightweight HTTP Server component vulnerability — remote unauthenticated; modify some data CVE-2026-91453
	JGSS component vulnerability — remote; create/delete/modify critical data CVE-2026-91462
	JGSS component vulnerability — remote; needs user interaction; read critical data CVE-2026-91463
	JGSS component vulnerability — remote; needs user interaction; read critical data CVE-2026-91464
	JSSE (TLS) component vulnerability — remote; modify some data CVE-2026-83376
	JAXP (XML) component vulnerability — remote; modify some data CVE-2026-87367
	Security component vulnerability — remote; modify some data CVE-2026-91333
	ImageIO component vulnerability — remote; read a subset of data CVE-2026-91334
	AWT component vulnerability — remote; needs user interaction; limited data read CVE-2026-91335

	Sound component vulnerability — remote; needs user interaction; partial DoS CVE-2026-91400
	JSSE (TLS) component vulnerability — remote; modify some data CVE-2026-91461

CCRs included in Release 4.15.3

Release **4.15.3** includes resolution for these CCRs:

IPM3-1500	Java GUI closes unexpectedly instead of presenting the appropriate communication error when port 6874 is opened and port 6875 is blocked.
IPM3-1488	Revert to the original behavior for submitting zip files by disabling the automatic unzip process when the environment variable PD_SKIP_ZIP_UNPACK is set to true.
IPM3-1506	The scroll bar in the Debugging PSF Printers section of the Web Management Interface does not appear in some cases.
IPM3-1517	Actual destination dropdown from Web GUI is not available when you open a queue in a new tab.
IPM-32380	When clearing the job-discard-time attribute, the Web GUI sends epoch time 0 to pdserver instead of unsetting the attribute, causing pdserver to discard the job immediately.

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.

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.

Okta® is a registered trademark of Okta, Inc. in the U.S. and other countries.

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.

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.