IPP Job Reprint Password
(REPRINTPWD)

Status: Stable\Interim

Abstract: This registration defines a new “job-reprint-password” operation attribute and associated semantics to provide IPP with a mechanism to support password protection for reprinting saved jobs.

This document is an IPP Registration. For a definition of an "IPP Registration Document", see:


This document is available electronically at:

This document may be copied and furnished to others, and derivative works that comment on, or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice, this paragraph and the title of the Document as referenced below are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

Title: IPP Job Reprint Password (REPRINTPWD)

The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make changes to the document without further notice. The document may be updated, replaced or made obsolete by other documents at any time.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights.

The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology that may be required to implement the contents of this document. The IEEE-ISTO and its programs shall not be responsible for identifying patents for which a license may be required by a document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention. Inquiries may be submitted to the IEEE-ISTO by e-mail at: ieee-isto@ieee.org.

The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its designees) is, and shall at all times, be the sole entity that may authorize the use of certification marks, trademarks, or other special designations to indicate compliance with these materials.

Use of this document is wholly voluntary. The existence of this document does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to its scope.

About the IEEE-ISTO

The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and
acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit:

http://www.ieee-isto.org

About the IEEE-ISTO PWG

The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit:

https://www.pwg.org

Contact information:

The Printer Working Group
c/o The IEEE Industry Standards and Technology Organization
445 Hoes Lane
Piscataway, NJ 08854
USA
List of Figures

Figure 1: IPP Job Save and Reprint..................................................................................7

List of Tables
1. Introduction

Users and network administrators are increasingly concerned about network and data security, and this extends to printing. Most all Users are familiar with sending a Job to a Printer and the Printer processing that Job fairly immediately. Some Printers support controlling the processing, and some do so using a “job password” that prevents the Job from being processed until the User provides that password on the Printer’s control panel to approve its release to processing. The IPP “job-password” operation attribute [PWG5100.11] and related attributes support this workflow in IPP provide support for this workflow. Some Printers also support saving jobs for later printing or re-printing. In certain cases there may be Users that wish to take advantage of both capabilities. Unfortunately however, since “job-password” is an operation attribute, and that Job’s processing is the act of saving the Job, the “job-password” attribute does not persist beyond its being saved. Therefore, in order for IPP to support scenarios involving a password protected saved job, IPP must be extended with new attributes that convey a Job password that persists beyond Job processing completion.

Some Printers also support saving Jobs for later printing or re-printing. This facility might be provided as a user-selectable feature at job creation time, for instance using IPP Job Save [PWG5100.11]. Or the Printer might be configured to save all Jobs for some period of time so they are available for reprinting, without requiring the User to overtly choose this at job creation time.

But as defined currently, the IPP defined to support these two features cannot be used together to support the “saved job with password” scenario without changing the defined semantics of the existing IPP attributes. The Printer could provide unique processing methodologies to cause the job password to persist, but doing so would violate backward compatibility with the expected semantic defined for the “job-password” operation attribute. This could lead to a discrepancy between the User's expectations and what the Printer produces.

This registration defines a new “job-reprint-password” operation attribute to support the “saved job with password” scenario.

2. Terminology

2.1. Protocol Roles Terminology

This document defines the following protocol roles in order to specify unambiguous conformance requirements:

Client: Initiator of outgoing IPP session requests and sender of outgoing IPP operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).
2.2. Other Terms Used in This Document

*User:* A person or automata using a Client to communicate with a Printer.

*Saved Job:* A Saved Job is a Retained Job that the Printer retains indefinitely (until removed by a Delete-Job or Purge-Jobs operation) so that a copy of it can be reprinted any time using the Reprocess-Job or Resubmit-Job operations, rather than aging the job out after an implementation-defined period. [PWG5100.11]

2.3. Acronyms and Organizations

*IANA:* Internet Assigned Numbers Authority, http://www.iana.org/


*PWG:* Printer Working Group, http://www.pwg.org/

3. **Rationale** Requirements for IPP Job Reprint Password

In the definition of IPP Job Save [PWG5100.11], a reprint means that a Job has been processed and reached the completed state, and the Job has been saved (implicitly or explicitly). To simply save a Job, the Printer "processes" the Job by saving it.
The “job-password” operation attribute was defined to prevent the Printer from processing the submitted Job until the matching password was provided to the Printer. Since it is an operation attribute, the “job-password” attribute is not supposed to persist beyond the execution of that operation.

If “job-password” is used with IPP Job Save, preventing Job processing will prevent the Job Save process from completing because the Job’s processing when Job Save is enabled is to save the Job.

Since the individual semantics of these IPP attributes cannot be used in combination with one another to provide support for the “saved job with password” scenarios described in section 3.1, this registration document defines new IPP attributes to enable IPP to provide that support.

3.1. Use Cases

3.1.1. Protecting a Saved Document with a Persistent Password

Wilma has authored a departmental policy document that she intends to save on her departmental MFD, to allow some of her peers to print copies as needed. But as the document contains sensitive information, Wilma wishes to only allow those who know the job’s password to re-print copies. She is familiar with providing a password when configuring a print job, and she is also familiar with configuring the job to be saved in the printer. In the print dialog used to configure the print job on her computer, Wilma provides a password, and also chooses to have the job saved. Wilma clicks “Print” and the computer submits the job to the printer. The printer saves the job content and protects it with the password provided.
3.1.2. Re-printing a Saved Job Via Printer Control Panel

Barney hears from Wilma that she has saved that document to the departmental MFD. Wilma tells Barney the job's name, and Barney then goes to the MFD and looks up the job. He taps on the control panel to have a copy printed, and is prompted to enter the job's password. He enters that on the control panel, and the MFD prints a copy. Barney collects it from the output bin and returns to his desk.

3.1.3. Re-printing a Saved Job Using An IPP Client

4. Barney sends an IM to Betty that Wilma has saved a job on the departmental MFD. Betty opens her computer's print system and browses the saved jobs on the MFD. She selects the job and clicks “Print” to have a copy made for her. A dialog is presented asking for the job's password. Betty types in the job's password, and the MFD prints a copy. She collects it from the MFD and returns to her office.

4.1.1. Exceptions

4.1.2. Unauthorized Re-printing Disallowed From Printer Control Panel

Harvey, an employee from another department, walks up to Wilma's departmental MFD. He navigates the MFD's control panel user interface and sees Wilma's departmental policy document listed on the control panel. He tries to get the MFD to produce a re-print. The MFD challenges Harvey for the reprint password; Harvey doesn't know it. The MFD won't re-print the document without receiving the reprint password, so Harvey walks away empty handed.

4.2. Out of Scope

The following are considered out of scope for this document:

1. How the Document or Documents in a Job are stored by the Printer
3. Mechanisms for supporting per-user credentials / access control list for releasing the stored job.
4. Remote access for reprint.

4.3. Design Requirements

The design requirements for this document are:

1. Use existing attributes or collections if possible.
2. Support at the least the fidelity supported currently by “job password” and "job-password-encryption"
3. Register all attributes and operations with IANA

The design recommendations for this document are:

1. Reusing UI controls with similar enough purposes so that the user doesn't need to be confused by e.g. needing to interact with different controls for different kinds of passwords.

5. New Operation Attributes For Existing Operations

5.1. job-reprint-password (octetString(255) | no-value)

The REQUIRED "job-reprint-password" operation attribute specifies the password the Printer requires before permitting the saved Job to be reprinted. The Printer permanently attaches the password to a saved Job [PWG5100.11]. The Printer MUST associate this operation attribute with the Job when the Job Creation operation includes this attribute in the operation request, for as long as the Job is retained and available for reprinting. A Printer that supports and accepts the "job-reprint-password" attribute MUST save any Job that is created using a Job Creation operation that includes the "job-reprint-password" operation attribute. This operation attribute is used as a request attribute for the Job Creation operations listed in section 6.1, and as a response attribute for the Fetch-Job operation [PWG5100.18]. A Client MAY provide a zero-length value or the 'no-value' out-of-band value to specify that no authentication is required to reprint the Job. The Printer MUST NOT allow access to the Job's stored "job-reprint-password" attribute via IPP Get-Jobs or Get-Job-Attributes operations, but SHOULD provide access via Fetch-Job [PWG5100.18]. More detailed information about IPP operations that can include this operation attribute in either a request or response are listed in Section 6.1 of this document. Challenge the User for this password to authorize reprinting that Saved Job if the value is a non-zero-length octetString.

The Printer MUST associate this operation attribute with the Job, and it MUST persist for as long as the Job is retained and available for reprinting. The Printer MUST NOT allow access to the Job's stored "job-reprint-password" attribute via IPP or any other protocol. IPP operations that can and cannot include this operation attribute are listed in Section 6.1 of this document. This attribute MUST NOT be included in any IPP operation responses.

A Client MUST NOT include the "job-reprint-password" operation attribute in an operation sent over an insecure IPP connection. This operation attribute MUST be present in the operation request if the "job-reprint-password-encryption" operation attribute is present in the operation request.
5.2. job-reprint-password-encryption (type2 keyword | name(MAX))

The “job-reprint-password-encryption” operation attribute specifies the hashing algorithm used to obfuscate the password to produce the value specified by the “job-reprint-password” operation attribute. This attribute is semantically equivalent to the “job-password-encryption” operation attribute [PWG5100.11]. This operation attribute is used as a request attribute for the Job Creation operations listed in section 6.1, and as a response attribute for the Fetch-Job operation [PWG5100.18]. The Printer attribute MUST NOT allow access to the Job’s stored “job-reprint-password” attribute via IPP Get-Jobs or Get-Job-Attributes operations, but SHOULD provide access via Fetch-Job [PWG5100.18]. More detailed information about IPP operations that can include this operation attribute in either a request or response are listed in Section 6.1 of this document. be included in any IPP operation responses.

The value of this attribute must be one of the values listed in the Printer’s “job-reprint-password-encryption-supported” Printer Description attribute. If the Client specifies a zero-length value or ‘no-value’ for “job-reprint-password” then the value of this attribute MUST be 'none'.

This Operation attribute MUST be present in the Operation request if the “job-reprint-password” operation attribute is present. The value of this attribute must be one of the values listed in the Printer’s “job-reprint-password-encryption-supported” Printer Description attribute.

Printer Description Attributes

5.3. job-reprint-password-supported (rangeOfInteger(0:255))

The "job-reprint-password-supported" attribute specifies the minimum and maximum length the Printer supports for the clear text unencrypted password. A conforming Printer MUST be able to accept 255 octets without truncation. However, a Printer MAY be implemented as a gateway to another print system that cannot accept the full 255-octet range, in which case the client MUST NOT allow an unencrypted password greater than the length specified by this attribute.

If the "job-reprint-password" operation attribute is supported, then this attribute MUST be supported.

5.4. job-reprint-password-encryption-supported (1setOf type2(type3 keyword | name(MAX)))

The "job-reprint-password-encryption-supported" Printer Description attribute specifies the encryption methods the Printer supports for obfuscating the value of the “job-reprint-password” operation attribute. The set of allowable keywords for this attribute are the same as those registered for the “job-password-encryption” attribute [PWG5100.11]. Deprecated keywords SHOULD NOT be listed.
If the Printer supports the "job-reprint-password" and “job-reprint-password-encryption” operation attributes, then this attribute MUST be supported.

5.5. job-reprint-password-repertoire-configured (type2 keyword supported (1setOf (type2 keyword))

The "job-reprint-password-repertoire-configured" attribute indicates the password repertoire currently configured for this Printer. The value of this attribute MUST be one of the set of values listed in the "job-reprint-password-repertoire-supported" attribute defined in 5.6. A supporting Client can use this attribute’s value to limit User input so that the value in "job-reprint-password" will comply with the configured password repertoire.

5.6. job-reprint-password-repertoire-supported (1setOf type2 keyword)

The "job-reprint-password-repertoire-supported" Printer Description attribute specifies the password repertoires (set of allowable characters) supported by this Printer for the "job-reprint-password-repertoire-configured" Printer Description attribute. A Client SHOULD use this attribute’s value to limit the range of allowable User input so that the value in "job-reprint-password" will be supported by the Printer. If the value of the “job-reprint-password” Operation attribute is encrypted, the Printer will be unable to reject the password at time of receipt, and the User may never be able to successfully authenticate to reprint the Job.

6. Additional Semantics For Existing Operations

6.1. Print-Job, Print-URI, Create-Job and job-reprint-password accesses

The “job-reprint-password” and “job-reprint-password-encryption” operation attributes MAY be included in a Print-Job, Print-URI, or and Create-Job operation request [RFC8011] to specify the persistent access credentials for a Job created by one of these operations. Although the “job-reprint-password” and “job-reprint-password-encryption” attributes get copied to the Job Object, the Printer MUST NOT include a Job’s “job-reprint-password” and “job-reprint-password-encryption” attributes in any Job-Description attributes in a Job operation such as Get-Jobs or Get-Job-Attributes [RFC8011].

6.2. Fetch-Job and job-reprint-password

The “job-reprint-password” and “job-reprint-password-encryption” operation attributes MAY be included in a Fetch-Job [PWG5100.18] operation response. The “job-reprint-password” and “job-reprint-password-encryption” operation attributes MUST NOT be included in a Fetch-Job [PWG5100.18] operation request.
7. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming implementations MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [STD63] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for Network Interchange [RFC5198].

Implementations of this specification SHOULD conform to the following standards on processing of human-readable Unicode text strings, see:

- Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical
- Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping
- Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]
- Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences
- Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization
- Unicode Collation Algorithm [UTS10] – sorting
- Unicode Locale Data Markup Language [UTS35] – locale databases

Implementations of this specification are advised to also review the following informational documents on processing of human-readable Unicode text strings:

- Unicode Character Encoding Model [UTR17] – multi-layer character model
- Unicode in XML and other Markup Languages [UTR20] – XML usage
- Unicode Character Property Model [UTR23] – character properties
- Unicode Conformance Model [UTR33] – Unicode conformance basis

8. Security Considerations

The IPP extensions defined in this document require the same security considerations as defined in the IPP/1.1: Model and Semantics [RFC8011], IPP: Job and Printer Extensions – Set 2 (JPS2) [PWG5100.11], and IPP Job Password Repertoire [IPPREPERTOIRE].

In addition to those requirements, the Printer MUST protect the values of “job-reprint-password-accesses” at rest. Also, the Printer MUST reject any IPP operation sent over a non-encrypted connection that includes the “job-reprint-password-accesses” attribute.

8.1. Human-readable Strings

Implementations of this specification SHOULD conform to the following standard on processing of human-readable Unicode text strings, see:
• Unicode Security Mechanisms [UTS39] – detecting and avoiding security attacks

Implementations of this specification are advised to also review the following informational
document on processing of human-readable Unicode text strings:
• Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

9. IANA Considerations

9.1. Attribute Registrations

The attributes defined in this document will be published by IANA according to the
procedures in IPP Model and Semantics [RFC8011] section 6.2 in the following file:
http://www.iana.org/assignments/ipp-registrations

The registry entries will contain the following information:

<table>
<thead>
<tr>
<th>Operation attributes:</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>job-reprint-password (octetString(255)</td>
<td>no-value)</td>
</tr>
<tr>
<td>job-reprint-password-encryption</td>
<td>[REPRINTPWD]</td>
</tr>
<tr>
<td>(type2 keyword</td>
<td>name(MAX))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Printer Description attributes:</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>job-reprint-password-supported</td>
<td>[REPRINTPWD]</td>
</tr>
<tr>
<td>(rangeOfInteger(0:255))</td>
<td></td>
</tr>
<tr>
<td>job-reprint-password-encryption-supported</td>
<td>[REPRINTPWD]</td>
</tr>
<tr>
<td>(isetOf type2(type3 keyword</td>
<td>name(MAX)))</td>
</tr>
<tr>
<td>job-reprint-password-repertoire-configured</td>
<td>[REPRINTPWD]</td>
</tr>
<tr>
<td>(isetOf type2 keyword)</td>
<td></td>
</tr>
<tr>
<td>job-reprint-password-repertoire-supported</td>
<td>[REPRINTPWD]</td>
</tr>
<tr>
<td>(isetOf +type2 keyword)</td>
<td></td>
</tr>
</tbody>
</table>

10. References

10.1. Normative References

https://ftp.pwg.org/pub/pwg/ipp/whitepaper/wp-job-password-
repertoire-20160101.pdf
"Information technology -- Universal Coded Character Set (UCS)",
ISO/IEC 10646:2011

Document Object”, PWG 5100.5-2003, October 2003,
http://ftp.pwg.org/pub/pwg/candidates/cs-ippdocobject10-20031031-
5100.5.pdf

T. Hastings, D. Fullman, "IPP: Job and Printer Extensions – Set 2
(JPS2)", PWG 5100.11-2010, October 2010,
https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-
20101030-5100.11.pdf

R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP Version 2.0, 2.1,
and 2.2", PWG 5100.12-2015, October 2015,

M. Sweet, I. McDonald, P. Zehler, "IPP: Job and Printer Extensions -
Set 3 (JPS3)", PWG 5100.13-2012, July 2012,
http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-
20120727-5100.13.pdf

M. Sweet, I. McDonald, “IPP Shared Infrastructure Extensions”, PWT
ippinfra10-20150619-5100.18.pdf

S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015,
August 2015, http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-
20150821-5100.19.pdf

R. Khare, S. Lawrence, “Upgrading to TLS Within HTTP/1.1”, RFC

R. Herriot, I. McDonald, “Internet Printing Protocol/1.1: IPP URL

J. Klensin, M. Padlipsky, “Unicode Format for Network Interchange”,

D. Hardt, “The OAuth 2.0 Authorization Framework”, RFC 6749,

Authentication”, RFC 7616, September 2015,
https://www.ietf.org/rfc/rfc7616.txt

J. Reschke, “The 'Basic' HTTP Authentication Scheme”, RFC 7617,

R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1):
Message Syntax and Routing", RFC 7230, June 2014,
http://www.ietf.org/rfc/rfc7230.txt
10.2. Informative References


11. Authors' Addresses

Primary authors:

Smith Kennedy
HP Inc.
11311 Chinden Blvd.
Boise ID 83714
smith.kennedy@hp.com

The authors would also like to thank the following individuals for their contributions to this standard:

Ira McDonald – High North Inc.
Mike Sweet – Apple Inc.

12. Change History

12.1. June 20, 2018

Added a figure to section 3 and also moved the new text from section 4 to section 3 because that is where it seems to fit best.

12.2. June 19, 2018

Updated as per feedback from the PWG May 2018 F2F

• Rewrote section 1
• Fixed title of section 3
• Removed section 3.1.3
• Added preamble text to section 4
• Updated Section 4 with a number of changes
• Added "job-reprint-password-repertoire-configured" to Section 5
497  • Added Fetch-Job to Section 6
498  • Added references to 5100.18 and IPPREPERTOIRE

499  12.3. April 24, 2018
500  Re-authored using the new PWG Working Draft template for Apache OpenOffice, moving
501  away from LibreOffice due to interoperability issues. Also, adopted changes recommended
502  in the April 12, 2018 IPP WG meeting:
503  • Returned to the “job-password” / “job-password-encryption” attribute set design
504  pattern from the “xxx-accesses” attribute set design pattern.

505  12.4. April 4, 2018
506  Updated as per feedback from IPP WG meeting on March 29, 2018
507  • Converted document to an IPP Registration document and made document
508  changes and file name changes to comply with that policy.
509  • Renamed “job-save-accesses” to “job-reprint-accesses”
510  • Removed “access-x509-certificate” but can add it back in later if its use becomes
511  more clearly defined

512  1.1 March 13, 2018
513  Updated as per feedback from IPP WG reflector:
514  • Fixed the abstract to make it less redundantly redundant.
515  • Fixed RFC references for HTTP Basic and Digest authentication
516  • Removed “job-save-accesses-configured” (but I still don’t understand why some use
517  the “xxx” / “xxx-supported” model while others use “xxx” / “xxx-configured” / “xxx-
518  supported”...) 
519  • Added new “Additional Semantics for Existing Operations” section
520  • Updated Security Considerations

521  1.2 March 11, 2018
522  Updated as per feedback from February 2018 PWG F2F review:
523  • Refactored the attributes used to leverage the attributes used in IPP Shared
524  Infrastructure Extensions and IPP Scan Service. This model is more appropriate
525  since job-save and its members become Job Description attributes, which are
required to be accessible via a Get-Job-Attributes operation. Access to the credentials, even if hashed, would be unacceptable.

• Propose this be moved to IPP Registration candidate status

1.3 February 5, 2018

Updated as per feedback from Dec. 14, 2017 IPP WG teleconference review:

• Updated Use Cases, Out of Scope and Design Requirements sections

• Refactored to make the solution become member attributes of job-save, with associated Printer Description attributes.

1.4 December 5, 2017

Initial revision.