AccurioPro Flux

Security whitepaper

For AccurioPro Flux version 10.4.2

Document revision: 0

Last modified: 11.05.2026

1 Preface 3
2 dots Software within the Konica Minolta compliance framework 3
2.1 Emergency response 4
2.2 Data protection (GDPR within the EU framework) 4
2.3 Information security incident management 4
2.4 Export regulations 4
3 Software development process 5
3.1 Product security 5
3.2 Quality assurance (QA) 5
4 AccurioPro Flux 6
4.1 System architecture 6
4.2 Flux Server: Security Architecture 7
4.2.1 Data storage 7
4.2.2 Transport security 7
4.2.3 Access control: Operator interface 8
4.2.4 Access control: Flux Printer Interface 8
4.2.5 Integration services API 9
4.2.6 Network security 9
4.2.7 Authentication / Configuration Logs 9
4.2.8 External interfaces 9
4.3 Flux Web: Security Architecture 9
4.3.1 Data storage 9
4.3.2 Transport security 10
4.3.3 Access control 10
4.3.4 General security measures 11
4.3.5 Authentication / Configuration Logs 11
4.3.6 External interfaces 11
4.4 Registration process 11
4.5 Analytics 11

1 Preface

AccurioPro Flux is a print workflow solution developed by dots Gesellschaft für Softwareentwicklung mbH (dots Software). We are a subsidiary of Konica Minolta Europe and develop software for digital printing since 1997.

AccurioPro Flux is used by thousands of customers worldwide. We not only strive for outstanding functionality and excellent usability in our product, but we also place great emphasis on its security.

This paper serves as a guide and overview of security measures we have in place for:

- Organizational processes
- Software development and quality assurance
- Product architecture

The provided information aims to help our vendors and customers to evaluate the security of our product and processes to ensure it matches their requirements.

2 dots Software within the Konica Minolta compliance framework

dots Gesellschaft für Softwareentwicklung mbH (dots Software) in Berlin, Germany is a Konica Minolta software development company operating within the compliance framework of Konica Minolta Europe.

We provide second level support to Konica Minolta sales companies worldwide and selected distributors for support cases connected to licenses with a valid Software Maintenance Plan (SMP).

We are regularly audited by the Quality Management Division of Konica Minolta Inc., guided by ISO 9001 principles.

Konica Minolta products, including AccurioPro Flux, use various technologies concerned with security topics. We rely on customers operating the products properly in accordance with the provided instructions. Please refer to the user manuals for proper setup and configuration of software and devices.

Before looking at how we design and develop our software in a secure way, some remarks on how we meet regulatory requirements in general:

2.1 Emergency response

Topics such as **Business continuity, Crisis management** and **Disaster recovery** are managed at dots Software in coordination with Konica Minolta Europe.

An **IT security policy** is in place to minimize the risk of compromising the development environment via malware, cyberattacks, etc.

2.2 Data protection (GDPR within the EU framework)

Data protection is managed in coordination with Konica Minolta Europe.

- Audited by Konica Minolta Europe in 2022.
- All employees are annually trained and sign a confidentiality agreement upon employment, before processing personal data.
- Actively maintained directory of processing activities is available.
- Privacy by design and default is implemented as principle in our development process (see Software Development process).

  A Data Processing Agreement between Konica Minolta Europe and dots Software is in place, which can be joined by the Konica Minolta sales companies on request.

2.3 Information security incident management

- We handle information security incidents according to our internal Information Security Policy and in coordination with Konica Minolta Europe.
- We maintain an information platform (dots Infohub) for the distribution of information, training, and updates to vendors of AccurioPro Flux.
- We inform our vendors about security updates related to incidents and vulnerabilities on dots Infohub or via newsletter.

2.4 Export regulations

- All non-open source third party components originate from the U.S. or the EU.
- Telecommunication or encryption software components are common open-source software (OSS).

3 Software development process

3.1 Product security

Our development is guided by the “security by design” approach. Threat modeling is performed based on the OWASP Top 10 for all features and self-developed software components. Mitigations are implemented for all identified threats.

Dedicated personnel oversee product security.

For every software release, automated penetration tests, dynamic security analysis, as well as scans for known vulnerabilities in used components are executed. Vulnerability databases are continuously monitored to be able to react to any newly discovered security vulnerabilities.

In case we learn about major security vulnerabilities in our software or used components, we will inform Konica Minolta sales companies via the dots Infohub and provide mitigations and software updates there. Additionally, the incident will be reported to the Konica Minolta Europe Computer Security Incident Response Team (BEU CSIRT).

Static code analysis tools are used during development to ensure code quality and adherence to secure coding standards.

For every version, all new and changed functionality is checked by our data protection coordination manager during the development process for compliance with common data protection legislation.

3.2 Quality assurance (QA)

Quality assurance is performed by a dedicated QA team on all AccurioPro Flux releases, to ensure functionality and stability.

The QA team collaborates with the Concept & Design team and the Development team to collect requirements and identify potential areas where errors might occur.

Based on the requirements, QA creates a test plan for every release as well as test cases for new features and functionality. Additionally, bugs to be fixed for upcoming releases are selected.

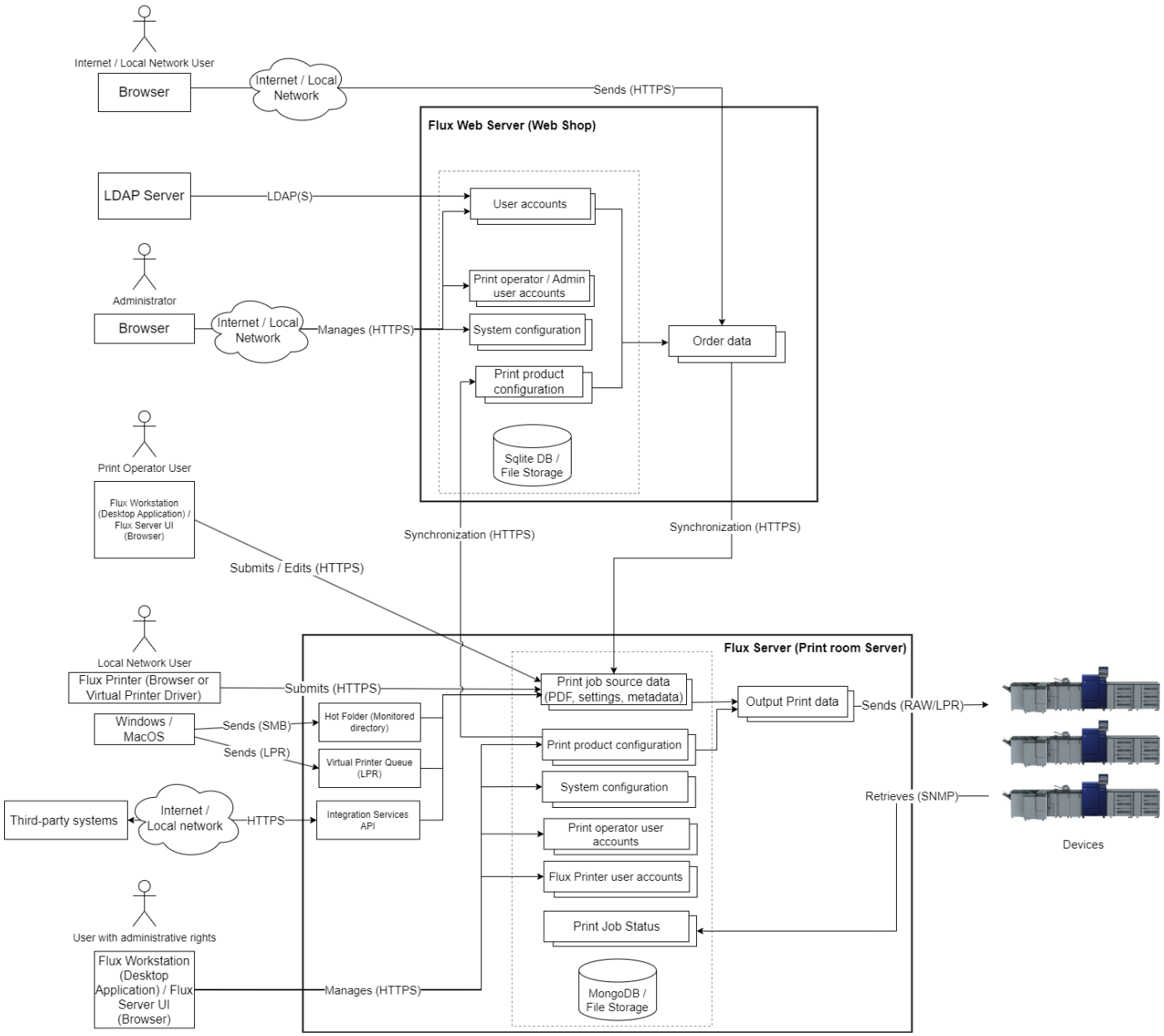
The software is then tested in multiple cycles (alpha, beta, final candidate), utilizing both manual and automated testing methods. After every cycle, quality requirements regarding functionality and detected errors must be achieved to move to the next cycle.

Once it is verified that all requirements are fulfilled and major bugs have been fixed, the new software version is released.

4 AccurioPro Flux

4.1 System architecture

AccurioPro Flux System Diagram



4.2 Flux Server: Security Architecture

4.2.1 Data storage

AccurioPro Flux utilizes a local MongoDB Community Server instance with network access limited to the server it is installed on.

Access to the database requires authentication. The corresponding authentication data is stored in the Flux Server configuration data and is inaccessible by non-administrator users on the same machine.

The following types of data are stored by Flux Server:

- **User Account Data:** Includes operator accounts as well as Flux Printer user accounts. Stored inside MongoDB. See the sections on access control below for details.
- **Print Order Data:** Source files for print jobs, usually PDF or PS files. Stored on the local hard drive.
- **Print Order Metadata:** Metadata for print jobs such as customer address data, delivery information etc. Stored inside MongoDB and an SQLite database (monitoring database).
- **Configuration data:** Configuration information such as print products, and credentials for connecting to LDAP, email server, etc. Stored inside MongoDB. Passwords for connecting to email and LDAP servers are stored in AES-encrypted form.

  For data stored on the local hard drive (such as print order data), operating system level access control can be used to limit access to the data on the device while it is active. Operating system storage encryption can be used to ensure data safety while the device is not in use.

4.2.2 Transport security

Communication between all clients (browsers, Flux Workstation, Flux Printer) and Flux Server can be encrypted by using TLS (HTTPS) connections. By default, only HTTPS is allowed for remote connections..

Communication between Flux Server and Flux Web can be encrypted by using TLS (HTTPS) connections. A user-supplied TLS certificate is required.

Note that data is encrypted in transport, but not at rest.

When using virtual printers, jobs are submitted to Flux Server via LPR, which is not encrypted.

When sharing hot folders via Windows file sharing, jobs are submitted over the SMB protocol, which supports encryption, depending on the capabilities of both Windows client and server.

4.2.3 Access control: Operator interface

The operator interface is the user interface for print operators, allowing management of print jobs and configuration of the AccurioPro Flux installation. It can be accessed via a web browser or the Flux Workstation desktop application.

Access to the Flux Server operator interface via a web browser or Flux Workstation is restricted to authenticated users. A valid combination of username and password is required for authentication.

- Passwords are stored in hashed form, using the Scrypt algorithm, with a unique salt per user account.
- Access to functionality is restricted by the rights granted to each user by administrators.
- Available rights are:
  - Edit/ Delete/ Assign Jobs
  - Folder Management
  - Print Room Setup
  - Manage User Accounts
  - Change System Administration Settings
- Administrative functionality can only be accessed by users that have the appropriate access right.
- Likewise, other configuration changes are limited to users with that access right.
- Print jobs can be viewed and printed by any logged in operator user.

4.2.4 Access control: Flux Printer Interface

The Flux Printer interface is the user interface for non-operator users which allows submission of print jobs to AccurioPro Flux. It can be accessed via a web browser or using the Flux Printer client.

Flux Printer users are managed separately from operator users and belong to a different user pool.

Access to the Flux Printer interface via a web browser or the Flux Printer client software is restricted to authenticated users. A valid combination of username and password is required for authentication.

Passwords are stored in hashed form, using the Scrypt algorithm, with a unique salt per user account.

Flux Printer users can also be managed via LDAP, in which case no passwords are stored in Flux Server.

Flux Printer users can only access those functions that are necessary for the ordering workflow to work.

4.2.5 Integration services API

Flux Server provides the Integration services API for integration with other systems. This API is disabled by default and requires an additional activation key to be enabled.

The API can only be accessed via HTTPS.

Authentication tokens are created by an administrator and must be sent with every request made to the API.

Access to job data can be restricted so that jobs created using a certain token can only be accessed using that token.

4.2.6 Network security

A full list of used ports and network protocols can be found in the Service Preparation Guide for AccurioPro Flux, available at the dots Infohub.

4.2.7 Authentication / Configuration Logs

Flux Server logs all authentication attempts, enabling the detection and investigation of potential unauthorized or malicious access.

In addition, all security-relevant configuration changes are recorded, ensuring a comprehensive audit trail of user activities and system modifications.

Logs are retained for a limited period to ensure that potentially sensitive data is not stored longer than necessary.

4.2.8 External interfaces

Flux Server provides several interfaces for communication from and to other systems, such as Hot folders and an LPR Server. By default, all interfaces which are not necessary for basic operation of the product are disabled to minimize any possible attack surface.

4.3 Flux Web: Security Architecture

4.3.1 Data storage

Flux Web, the web server running the web shop available in AccurioPro Flux Ultimate, stores data on the local hard drive in an SQLite database as well as separate files.

The following types of data are stored by Flux Web:

- **User Account Data:** Includes operator accounts as well as Flux Web user accounts. Stored inside the SQLite database. See the section on access control below for details. Note that operator accounts in Flux Web are independent from operator accounts in Flux Server.
- **Print Order Data:** Source files for print jobs, usually PDF or PS files. Stored on the local hard drive.
- **Print Order Metadata:** Metadata for print jobs such as customer address data, delivery information etc. Stored inside SQLite DB.
- **Configuration data:** Configuration information such as print products and credentials for connecting to LDAP, email server, etc. Stored inside configuration files on the local hard drive. Passwords for connecting to email and LDAP servers are stored in AES-encrypted form.

  Operating system level access control can be used to limit access to the data on the device while it is active. File system level storage encryption can be used to ensure data safety while the device is not in use.

4.3.2 Transport security

Communication between all clients (browsers, Flux Server and Flux Web Printer) and Flux Web can be encrypted by using TLS (HTTPS) connections. By default, TLSv1.2 and TLSv1.3 are enabled, and older protocol versions are rejected.

By default, Flux Web sets the “secure” cookie flag, therefore only allowing logging in via HTTPS connections, except for local connections from the server itself. HTTP can be disabled altogether in the configuration.

4.3.3 Access control

Access to the Flux Web server interface via a web browser is restricted to authenticated users.

Users can be managed via the local Flux Web database or via an external authentication provider (SAML, IWA, LDAP).

If managed locally, passwords are stored in hashed form (Scrypt) only, with a unique salt per user account. Otherwise, passwords are not stored within Flux Web.

The minimum password length is configurable in the Flux Web administration user interface.

For configuring more detailed password requirements, refer to Technote #10-46, available at the dots Infohub.

Users’ access to functionality is based on their user role. The membership in user roles is controlled by the administrator.

Administrative functionality can only be accessed by users that have the appropriate user role.

4.3.4 General security measures

Input validation and parametrized queries are employed to prevent injection attacks, which occur when untrusted data is inserted into a command or query.

The provided standard configuration is kept as secure as possible to ensure that a default installation is not vulnerable against any attacks.

4.3.5 Authentication / Configuration Logs

Flux Web logs all authentication attempts, enabling the detection and investigation of potential unauthorized or malicious access.

In addition, all security-relevant configuration changes are recorded, ensuring a comprehensive audit trail of user activities and system modifications.

Logs are retained for a limited period to ensure that potentially sensitive data is not stored longer than necessary.

4.3.6 External interfaces

Flux Web provides several interfaces for communication from and to other systems, such as an LPR Server. By default, all interfaces which are not necessary for basic operation of the product are disabled to minimize any possible attack surface.

4.4 Registration process

To use the software, it must be registered by entering the serial number, the customer's company name, email address and the sales contact email address.

All data is transferred via TLS (HTTPS) to the dots license server. The server is located in Germany.

4.5 Analytics

AccurioPro Flux may transfer usage data to dots Gesellschaft für Softwareentwicklung.

All usage data is transferred via TLS (HTTPS) to the dots analytics server. No personally identifiable information or sensitive data is transmitted. The server is located in Germany.

For more information, please refer to https://accuriopro-flux.com/analytics.

All information for this documentation has been compiled with care, but is provided without warranty of any kind.

No portion of this documentation or the program may be reproduced or distributed on electronic or other media in any form (print, photocopy, microfilm or other method) without the prior written permission of dots Gesellschaft für Softwareentwicklung mbH.

AccurioPro is a trademark of Konica Minolta, Inc. All other brand names and product names belong to the respective companies and are protected by international trademark, brand and patent laws.

All rights reserved.



dots Gesellschaft für Softwareentwicklung mbH
Schlesische Straße 27 | 10997 Berlin | Germany
info@dots-software.com | www.dots-software.com



Konica Minolta Business Solutions Europe GmbH
Europaallee 17 | 30855 Langenhagen | Germany
Phone +49 (0) 511 74040 | www.konicaminolta.eu