Secure by Default
Protecting your Business and Information

uniFLOW

RYAN
Business Systems, Inc.

ryanbusiness.com 800.842.1916

Highest Security Standards

Award-winning Secure Print features are the most valuable components of uniFLOW, ensuring printed documents are released only to designated employees, but there are more aspects to information security than just printed copy.

Secure by default

The key to ensuring a secure system is to start off with high security and then tone down security settings where necessary. To this end uniFLOW is installed with security features such as the encrypted web server turned on plus the option to moderate security where it is not needed.

End to End Security

Security is considered across all functionalities offered as part of the uniFLOW Platform. Infrastructure plays a big part in securing a software product but security can be enhanced by applying extra features and functionalities.

Testing our Resolve

Security threats are constantly evolving and becoming more sophisticated. uniFLOW is written with a 'Secure by default' approach to all development. This means employing best practice in development and the OWASP Top 10 for Security. Penetration testing is performed during the development cycle using security tools such as BURP. Testing is continued in the QA process where uniFLOW is security reviewed internally and by an independent external security organisation.
All security threats identified in QA or from the field are acted upon with the highest priority to ascertain the threat and fix accordingly. With every release of uniFLOW it is also independently audited by and external company.

Secure Platform

uniFLOW brings together and simplifies many technologies through a common program and interface. An important aspect to this is retaining security across these components.

How does uniFLOW instill confidence in your input and output management infrastructure?

- Secure network communication
- Control device access and certain features
- Print job security
- Secure print mobility options
- Scanning securely, also from cloud services
- Audit document activity


Security
Impacts
Business

How can uniFLOW help?

Communicate with Confidence

Whilst integral to network and information security, perimeter defence does not provide sufficient protection for all your information. Unintentional data leakage and malicious breaches are real threats and you should assume they are already inside your network.

Consequently communication across connected servers and devices needs to be secure whatever the size of your network. Straight out of the box, uniFLOW ensures information is securely communicated between its various components.

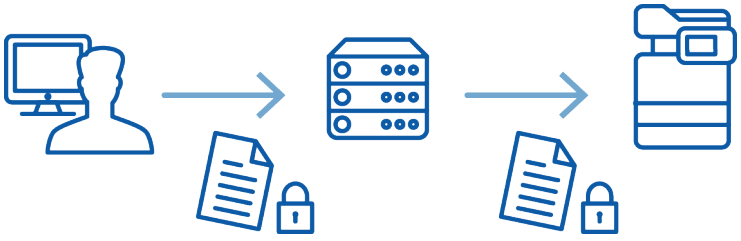
uniFLOW provides additional layers of security when transmitting print jobs across a network by encrypting the data. While jobs are in transit through a network and susceptible to interception, they remain encrypted until they reach the device from where they can be securely released.

"I need to ensure all network communication is secure and protected against malicious and unintentional data breaches."

Frank (IT Manager)

How can uniFLOW help Frank?

Print Job Encryption: Encryption of print jobs in transit using AES-256 respectively RSA encryption.



Device Access Control

Devices are generally the end point in the printing process, producing the fi nal output. These devices can open up your organization and infrastructure to malicious attack and misuse. uniFLOW provides a detailed layer of security to control both device functions and user access.

"How can I secure individual device features against abuse or misuse in corridors and public access areas?"

Helen (Finance Director)

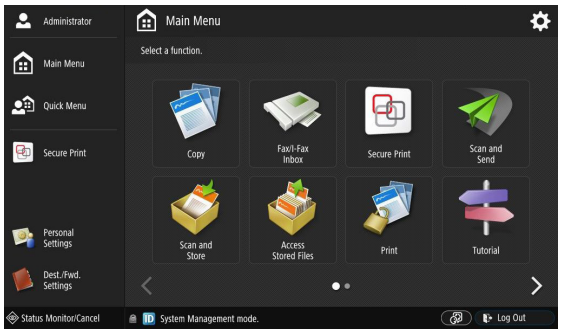
How can uniFLOW help Helen?

Authentication

- Diverse authentication options including proximity card, magnetic swipe card, username/password or PIN code
- Can work with any networked printer

Access Management Service (AMS)

- User device level security of key functions
- Block print/scan by USB for unauthorized users
- Restrict access to the internal email address book
- Restrict access to Send to Myself and Scan to my Folder function



Guest Access

- Provide secure release of guest print jobs while maintaining device level security

Print with Confidence

The secure printing functionality allows all users to send their confidential documents to network printers from their desktops or mobile devices. The print job will only be printed when they are physically standing at the device.
Devices may error or run out of paper whilst printing a secure job. The print job is still being processed at the device and will complete when the error is cleared or paper is added. Human nature being what it is, users may not resolve these problems, choosing instead to release their job from another device. This exposes your organization to risk as the next person to correct the error or add paper will trigger the release of the remaining pages of the user previous printing.

uniFLOW can prevent this from happening by automatically deleting print jobs that are retained in the device upon a user logging out.

"If we only have utility room devices how can I ensure my print job security?"

Colby (Employee)

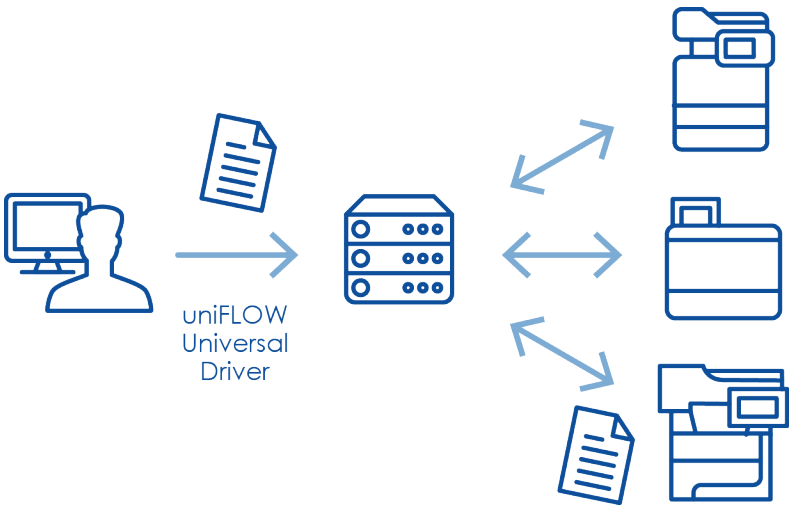
How can uniFLOW help Colby?

Automatic Device Error Job Deletion:

- uniFLOW can check whether a device is in error and, if the user is logged out, automatically delete the remaining print jobs
- Alternatively the user can be contacted via email, with the print job and device details, to make them aware that the error occurred

My Print Anywhere:

- Secure and convienient release of print jobs
- Multiple forms of user authentication
- Jobs available across multiple servers and sites



Mobility with Confidence

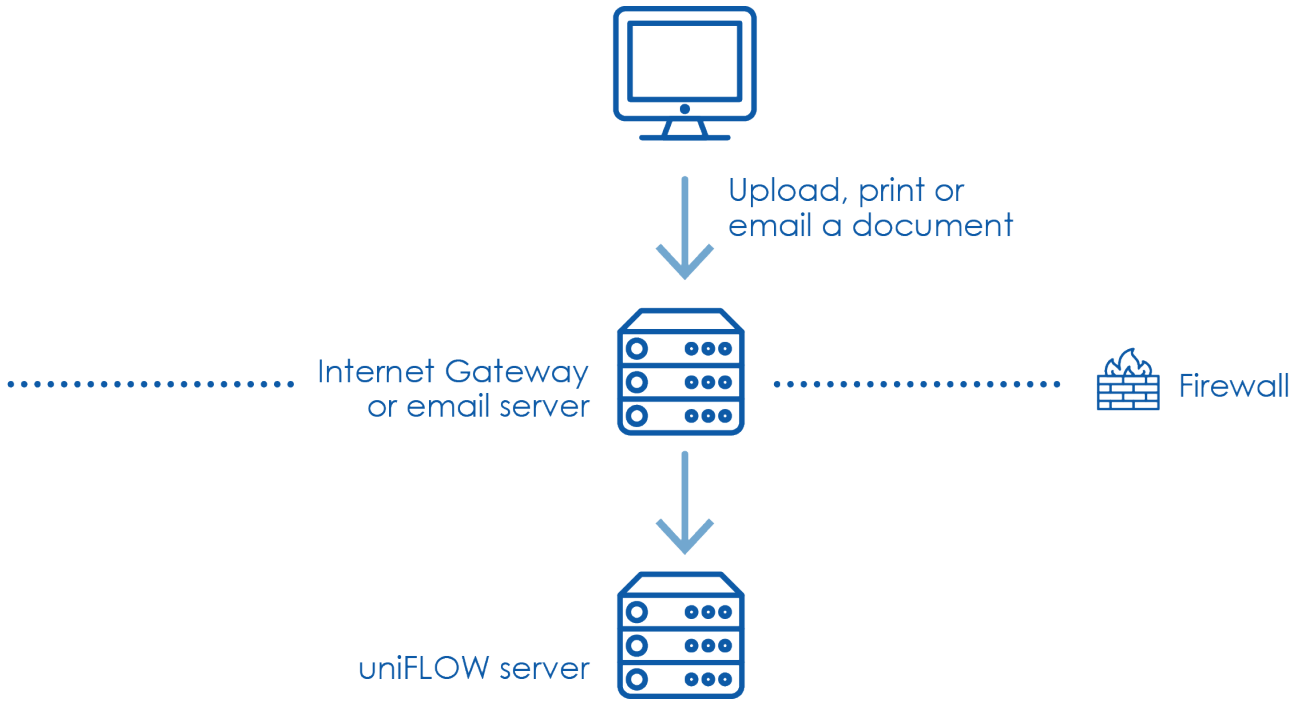
uniFLOW addresses common security risks for mobile and guest printing by providing external job submission pathways via email or web. This minimizes attack vectors by removing the need to add unknown/ unauthorized mobile devices to the organizational network.

"If users send mobile print jobs from outside the network, how can I ensure corporate security policies are followed?"

Stephanie (Marketing Manager)

How can uniFLOW help Stephanie?

- Mobile print jobs submitted via email already meet your organization's anti-virus, content policy and security rules
- Enterprise-wide Google Cloud Print™ converts all files via the Google cloud to a printable PDF format which is transferred securely to uniFLOW for processing
- The uniFLOW Internet Gateway allows for secure job submission via upload or native driver (Windows® and Mac®) to uniFLOW over SSL encrypted communication



Scan with Confidence

Scanning paper documents in the digital world is common practice. uniFLOW provides a powerful scanning and workflow engine to digtalize your documents. With digitalization comes distribution, often to external organizations across unfamiliar networks.

While uniFLOW can scan documents to many different file formats, PDF is universally recognized as the 'Portable' file format of choice. uniFLOW supports several PDF versions and standards. It can also produce encrypted PDFs with optional password-protection against viewing, editing or printing.

"I often scan documents to various locations for managers and clients. How can I ensure this is done securely?"

Ben (Marketing Assistant)

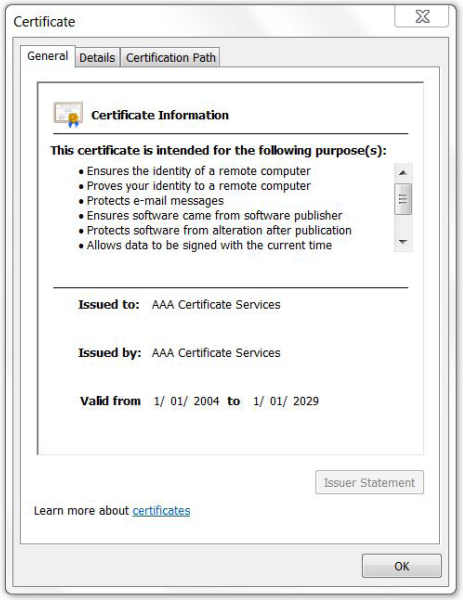
How can uniFLOW help Ben?

Secure Scan Destinations:

- For cloud service end-points 0Auth identity providers are supported
- User identities and credentials are stored securely with AES-256 encryption
- Access Control Lists ensure scan destinations are available to authorized users only

Secure Document Scanning:

- Security for PDF output is granted through password protection and certificate-based signing
- For PDF output meta-data support allows tracking for author and ownership
- All user scanning can be tracked, traced and reported



The ability to apply a signed digital certi fi cate to a PDF ensures authenti city for the receiver of a shared fi le.

Audit all Device Activity

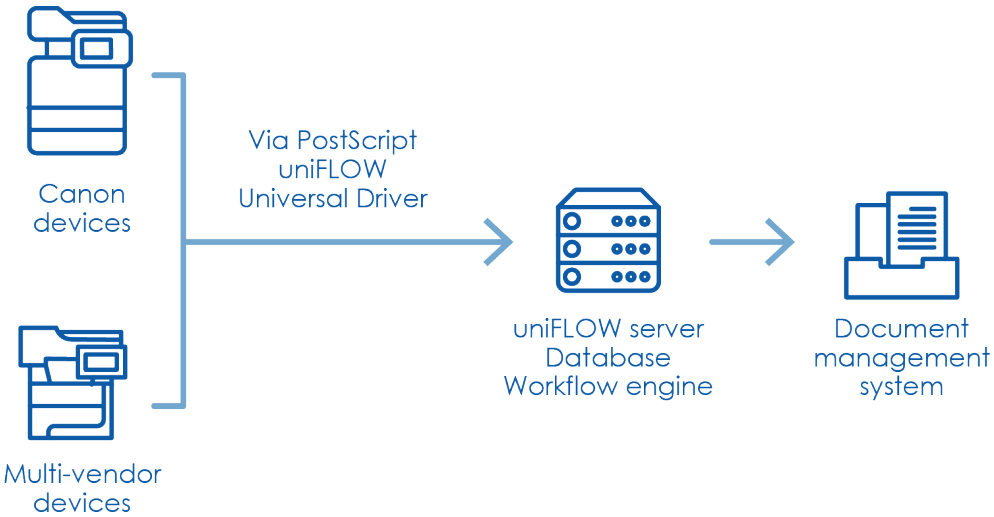
With the tight integration between uniFLOW and Canon's iW SAM Express, organizations can easily capture and archive all imaging activities such as print, scan, fax, copy and email. Each time an activity is performed on a Canon multifunctional device, the text data and image data can be captured together with log information to facilitate detailed auditing and flagging of confidential information for review. All data and images can be exported to a data loss preventi on system. Image and print data captured by iW SAM is processed by uniFLOW with the workflow engine allowing custom actions to meet business and security auditing requirements. Captured documents can be securely stored in a wide range of document management systems for later review.

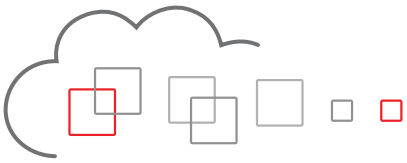
"Can I monitor all copy, fax, scan and print activity of devices where IP and sensitive information might be copied/scanned or faxed externally?"

Riccardo (Account Manager)

How can uniFLOW help Riccardo?

- Capture, audit and archive data and user information for print, copy, scan and fax jobs (text data, image data, log information)
- Print data can additionally be captured across multiple manufacturers when using the PostScript uniFLOW Universal Driver
- Notify a designated administrator when a specific keyword is printed, scanned, faxed, copied or sent so he/she is aware of crucial information leaks as they occur
- Full text search capability utilizing uniFLOW's OCR engine
- In conjunction with uniFLOW all captured data can automatically be exported to external DMS systems as well as data loss prevention systems





www.uniflow.global
www.uniflowonline.com

V3 | March 2019