AccuRoute

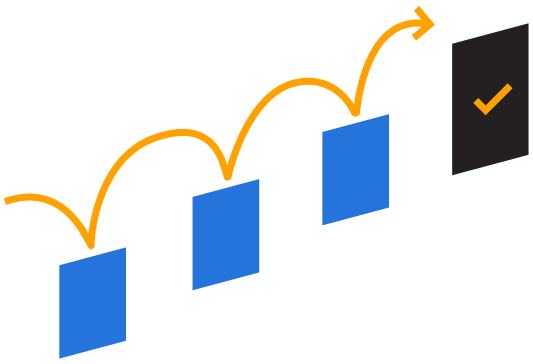
Protect your data with AccuRoute Content Monitor

We provide organizations with a way to easily monitor documents traveling through their enterprise for sensitive or confidential information.

By using specific rule sets, AccuRoute Content Monitor can execute workflows based on the information it finds to protect sensitive information from leaving the organization—or at a minimum, the ability to trace that information.

This robust solution gives users the ability to:

- Search and detect key terms or sequences in scanned, faxed, or printed (if they pass through AccuRoute) documents that may indicate the presence of confidential information or sensitive data
- Configure specific workflow rules for each flagged term
- Review flagged documents and related rule sets
- Create gated security blocks for sensitive data



Benefits

- Protect sensitive organizational, customer, and vendor data
- Facilitate data loss detection and prevention
- Prevent both intentional and unintentional data leaks
- Reduce time spent hunting for data or correcting errors
- Perform secure scans to detect data loss

Content Monitor Profiles

To protect data, organizations need the ability to differentiate day-to-day communications from those that contain sensitive data (i.e., a marketing datasheet vs. a confidential financial document). AccuRoute Content Monitor transforms the content of documents to text-searchable information to immediately detect key terms or numeric patterns that may indicate the presence of confidential or sensitive data.

- Detect certain words and phrases (i.e., "secure", "private", or "confidential") and specific character patterns such as credit card numbers or Social Security Numbers
- Support "fuzzy logic" functionality to detect data whether its uppercase, lowercase, or substituted numbers or symbols for a character (i.e., “s3cure” rather than “secure”)
- Utilize the Optical Character Recognition (OCR) engine already embedded in the AccuRoute platform for enhanced scalability for any organization’s needs
- Detect any supported languages added to the AccuRoute server using OCR

AccuRoute Preview and Self-Policing

Exposure to sensitive data varies depending on an employee’s roles and responsibilities. Though some staff encounter sensitive data on a regular basis, not every employee needs strict standard processes set for them as they may not deal with sensitive data often. When paired with AccuRoute Content Monitor, AccuRoute Preview allows system administrators to provide access to sensitive data to users on an as-needed basis. Give users the ability to:

- Quickly confirm the quality of the image
- Simply view the scan with no metadata entry or editing needed
- Note any flagged data highlighted in preview
- Immediately approve or reject data
- Work in conjunction with AccuRoute Content Monitor to create a self-policing workflow for data loss detection

In today's business climate, data security and compliance are more critical than ever. The almost daily reveal of significant security breaches around the globe coupled with the ever-growing instances of compliance and regulatory requirements are driving more stringent security requirements of technologies that handle sensitive information.

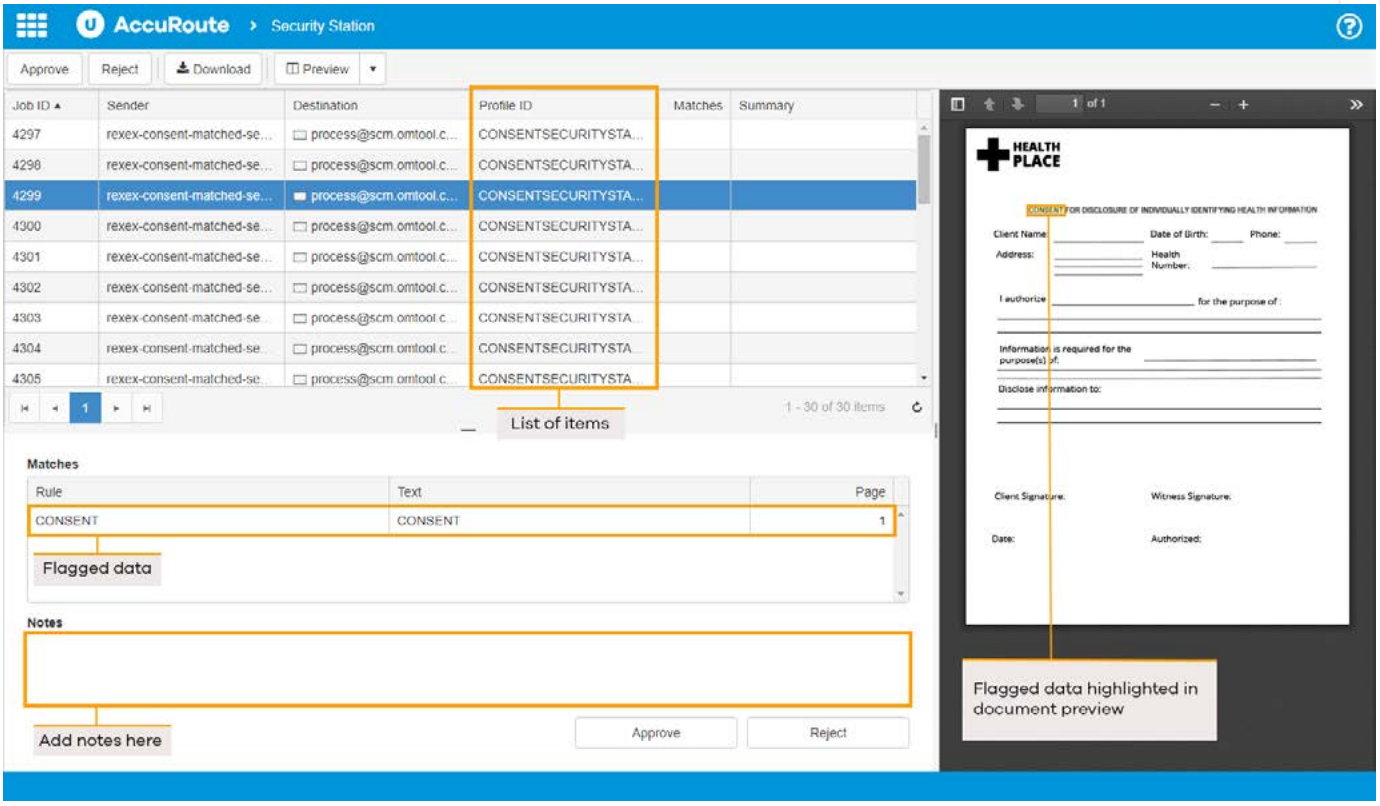
Shawn Freligh
EVP and General Manager, Upland Software

AccuRoute Security Station

The system administrator oversees much of the functionality of AccuRoute Content Monitor; however, delegated content auditors or end users are also able to intuitively interact with the module via the AccuRoute Security Station found in AccuRoute WebApps.

This simple dashboard allows users to:

- Easily locate sensitive data that has been flagged
- Quickly approve or reject flagged data
- Communicate specifics by adding a note



Ready to get things done?

Let us show you what AccuRoute can do.

Request a Demo

Upland AccuRoute helps organizations accelerate business processes by allowing users to easily capture, process, deliver, and fax content from any device using a single, unified platform. AccuRoute automates data capture and extraction using optical character recognition (OCR) to securely process through workflows to applications, people, or storage.