Giving Shape to Ideas

DocAudit™

Data and Document Protection for MFP Activities

DocAudit provides organizations an extra level of data and document security at their Konica Minolta MFPs

prism software

DocAudit™

DocAudit protects your confidential data and documents by providing real-time notifications of data breaches that occur with any MFP activity. It also provides a secure audit trail along with a text-searchable PDF of all bEST-enabled Konica Minolta MFP activities.

DocAudit assists organizations achieve compliance with industry and government requirements for privacy and data security.

DocAudit Protects Your Confidential Data

DocAudit creates a record of any Konica Minolta MFP user activity: Copy, print, scan, fax, and email. This record contains both the MFP user and device data as well as a text-searchable PDF copy of the MFP activity. This record is then automatically deposited into a secure database and document archive that is accessible only by permitted users.

DocAudit also provides real-time alerts in the event of a data breach at the MFP. The user predefines the data and keywords that constitute such a breach and DocAudit provides an alert should it find a match for that data or keyword. This alert provides the specific who, what, when, and where of such data breach.

Customize with Your Keywords & Data

Each organization can define temporary or permanent data and keywords that constitute a breach. Keywords and data patterns can be entered singly or batch-imported.

Data Patterns include:

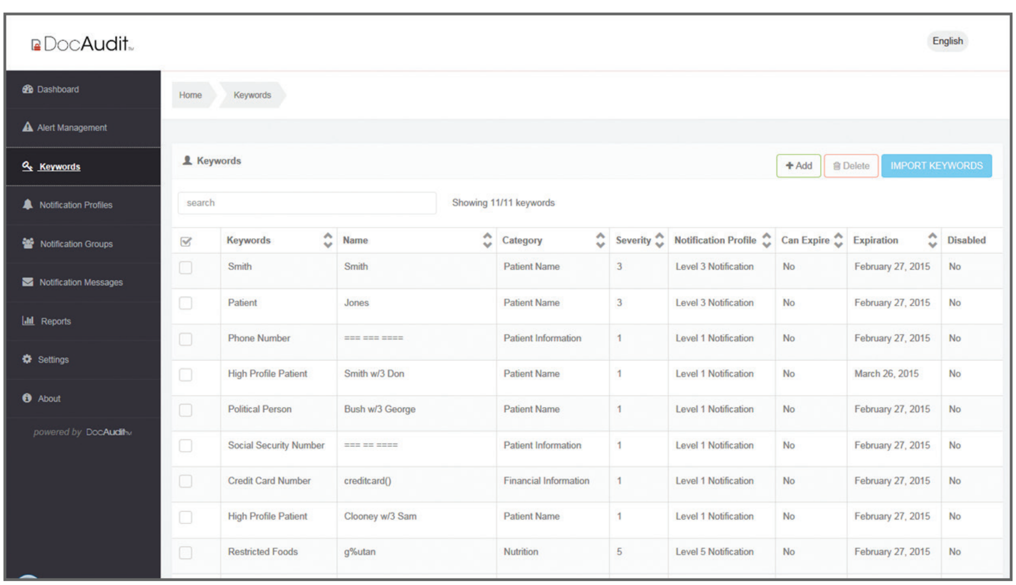
- *Social security numbers*
- *Credit card and patent numbers*
- *Phone numbers and dates*
- *IDs of patients, students, employees, and others*
- *Email addresses and URLs*
- *Much more*

Keywords include:

- *Names of patients, students, employees, and others*
- *Product or trade names*
- *Compliance terms*
- *Discrimination terms and phrases*
- *Disparaging phrases*
- *Much more*

DocAudit has a wide range of search criteria for data and keywords including:

- *"All words" and "Any words"*
- *Words and phrases*
- *Boolean*
- *Wildcards*
- *Fuzzy*
- *Phonic*
- *Stemming*
- *Synonym*
- *Number range*
- *Field*



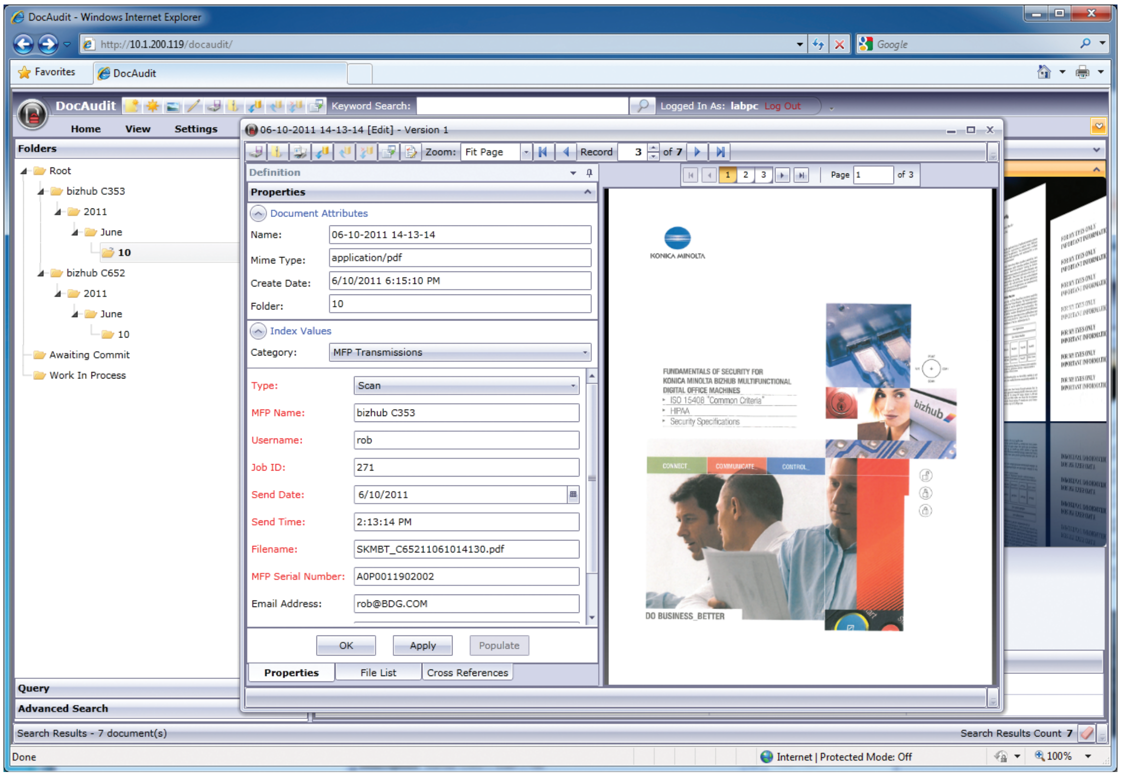
Easy-to-use and configure interface for entering and managing keywords and data patterns

Industries

Healthcare
Insurance
Government
Financial
Banking
Manufacturing

Administrators Can View Records Anywhere

All Konica Minolta MFP activities, along with the text-searchable PDFs of such activities, are securely stored in the DocAudit secure database. This is searchable by an authorized administrator who can access through an Internet browser or Windows-based desktop client. The Internet browser viewer works on Windows, Mac or Linux operating systems. Records are instantly available and documents can be easily and quickly previewed and retrieved.



Browser-based viewer for Windows, Mac, and Linux platforms

Configuration

DocAudit is easy to set up and use. It can handle up to thousands of Konica Minolta MFPs. Any Konica Minolta networked MFP equipped with ILTF can be configured to automatically output to DocAudit.

Key Features

- *Provides secure and searchable audit trail of all MFP activities*
- *Real-time breach alerts of user-defined keywords and data patterns*
- *Securely view audit records through either a desktop client or browser-based client*

Key Benefits

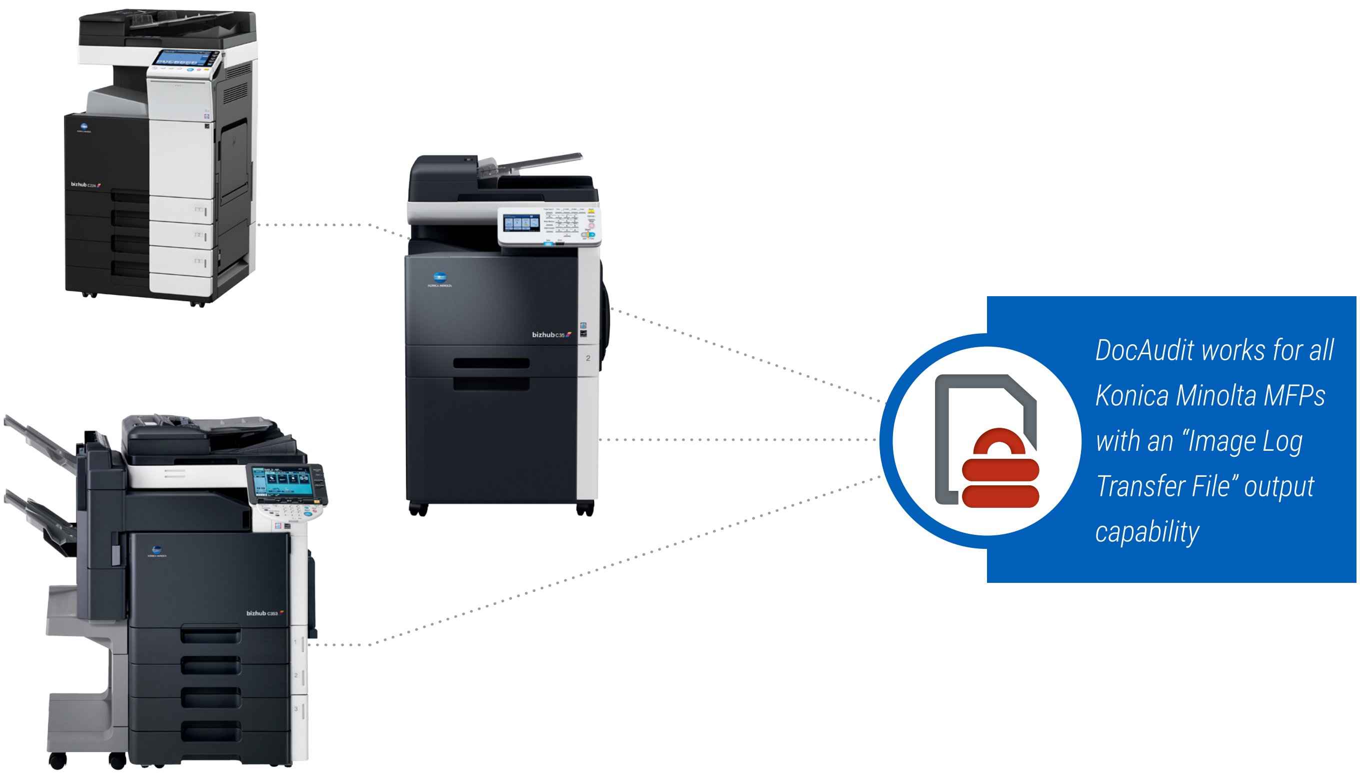
- *Assists organizations with data and privacy compliance regulations*
- *Provides real-time data and document breach alerts*
- *Greatly reduces sensitive data and documents being sent to unauthorized persons*
- *Provides a secure and searchable audit trail of all MFP user activities*

How it Works

Konica Minolta MFPs can automatically output their activity log ("Image Log Transfer File" or "ILTF") along with a PDF of that activity. This PDF and activity log are then automatically captured by DocAudit. The PDF is OCRed (optical character recognition) by DocAudit and becomes full-text searchable. The data from this activity log is indexed and archived in either a default format or user-defined format and the full-text searchable PDF is filed with it. DocAudit then compares the data in each OCRed document against the user-defined keywords and data patterns to see if there is a match. If there is a match, the user is notified.

DocAudit breach alert notifications and audit trail variables include:

- *Document name*
- *File type*
- *Creation date*
- *Type of activity*
- *MFP name*
- *User name*
- *Job ID*
- *Send date, time*
- *File name*
- *MFP serial number*
- *Email address*
- *More...*



15500-C Rockfield Blvd. Irvine, CA 92618 USA
(949) 855-3100 (949) 855-6341 fax
www.prismsoftware.com sales@prismsoftware.com

Konica Minolta Business Solutions (Canada) Ltd.
5875 Explorer Drive, Suite 100, Mississauga, Ontario L4W 0E1
www.kmbs.konicaminolta.us
www.kmbs.konicaminolta.us/solutions

Item#DocAuditBro
09-2016