KONICA MINOLTA

TECHNOLOGY

Dispatcher Phoenix

Security

Dispatcher *Phoenix*

White Paper

Table of Contents

90%

of U.S. organizations experienced leakage or loss of sensitive or confidential documents over the past 12-mark period

"Document Security and Compliance"
InfoTrends, April 2013

Introduction

The advancement of technology has transformed the MFP into a key element of a company's document infrastructure and workflow; however, as the role of the MFP has changed, the risk of security breaches has increased as well. Ensuring document confidentiality, allowing for system authentication, and providing clear audit trails are now necessities in every document-intensive industry. The objective of this white paper is to describe how Konica Minolta's Dispatcher Phoenix software application helps organizations comply with their security requirements.

Dispatcher Phoenix is a family of advanced document workflow products that streamline and automate document processing tasks, such as forms processing, file conversion, redaction, metadata routing, document indexing/folder browsing, etc. With a Dispatcher Phoenix secure workflow, documents can be captured from a variety of sources, processed, and then distributed to multiple locations, all at the same time. Dispatcher Phoenix is fully integrated with the MFP, allowing users to scan, index, process, and route their paper-based documents directly from the MFP.

To help organizations meet the compliance requirements for audit or security and ensure that their documents meet the security requirements of your organization, Dispatcher Phoenix was developed to follow Windows' best security practices. Dispatcher Phoenix is currently being used in a variety of industries that must follow stringent security standards, such as financial services, law firms, healthcare organizations, education, insurance, and government agencies. The Dispatcher Phoenix approach to security provides an ideal and unique way to protect or share sensitive information.

Why Security Matters

Although today's MFP is considered to be the central document processing hub for the workplace, facilitating the sharing of both digital and paper-based documents, this technological advancement has come with inherent and potential security vulnerabilities. Digital documents can be exposed. Critical business documents could be scanned and routed to unauthorized individuals. In general, any MFP application solutions must sure that their electronic access points are securely controlled and protected.

Although today's MFP is considered to be the central document processing hub for the workplace, facilitating the sharing of both digital and paper-based documents, this technological advancement has come with inherent and potential security vulnerabilities. Digital documents can be exposed. Critical business documents could be scanned and routed to unauthorized individuals. In general, any MFP application solutions must sure that their electronic access points are securely controlled and protected.

Add to that the fact that government mandates and regulations for providing customer/consumer privacy are affecting many companies. Financial services need to secure their financial records. School systems must protect student confidentiality. Hospitals and clinics must meet new healthcare security requirements. And confidentiality is critical for records and files in every law firm and legal department.

Konica Minolta has been at the forefront of developing and implementing security-based information technology in our MFPs to ensure that important information assets are protected from theft or loss. Konica Minolta understands that the best security solution is one that protects business information through every stage of the scanning process.

EXAMPLES OF SECURITY MANDATES

Health Insurance Portability and Accountability Act (HIPAA) protects private medical data

Gramm-Leach-Bliley Act requires financial institutions to implement appropriate safeguards to preserve the privacy of their customers' information

Family Education Rights and Privacy Act (FERPA) is designed to improve student privacy

That is why Dispatcher Phoenix, a Konica Minolta-developed software application, was designed to follow strict security guidelines and properly safeguard documents throughout the workflow.

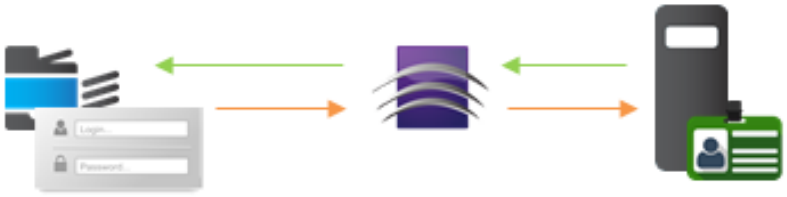
Controlling Access

User Authentication and Authorization

In security-conscious environments with shared devices, it becomes critical to limit device access to valid users only. User authentication must be implemented to verify the identity of the person accessing workflows at the MFP. With Dispatcher Phoenix's direct integration with Windows Authentication and Active Directory, explicit control over local and network resources is ensured. Dispatcher Phoenix offers robust and flexible authentication options for your document workflows. These options ensure that Dispatcher Phoenix workflows are run by valid and authorized users and that access to specific destinations are properly restricted.

Authenticating with username and password

Users can log into Dispatcher Phoenix using their Windows or Active Directory credentials. Once they have logged in successfully to Dispatcher Phoenix, they'll have immediate access to their workflows and personal scan destinations (e.g., home folders). For example, authenticated users can access their Scan to Email with LDAP workflow to seamlessly scan, process, and email scanned documents to the appropriate LDAP user.



Single sign-on authentication

Dispatcher Phoenix also offers single sign-on authentication where users are automatically logged into Dispatcher Phoenix as the user who is logged into the MFP. The MFP authenticates the user first and then sends that information to Dispatcher Phoenix.

Card Registration Tool

ID card registration from Dispatcher Phoenix Web speeds the use of card registration at the MFP. This easy-to-use, online Card Registration Tool allows administrators to quickly register ID cards using LDAP to their Active Directory or Novell eDirectory servers. This tool allows for easy registration of the most popular cards, such as HID Proximity, iCLASS and MIFARE, etc., using USB card readers like Konica Minolta's AU-205H. This tool also provides card lookup functionality so that administrators can quickly see who a card has been registered to, just by tapping the card on the card reader. Once cards have been registered, they can then be used to log into the MFP as well as Dispatcher Phoenix.

Limiting Workflow Access

In addition to Dispatcher Phoenix's support for user authentication, administrators can grant authorization to specific users or groups of users in Active Directory. The Dispatcher Phoenix Web interface includes a "Workflow Sharing" tool that is used to grant either view-only or edit workflow permissions to individual users or user groups. This provides the fine-grain control administrators need to ensure that only authorized staff members have rights to particular workflows.

Windows Impersonation

Applications are often configured to use accounts that are granted more privilege than is actually required. And, running as an administrator can be a risky practice, leaving your system vulnerable to security risks and exploits. When applications are allowed to run with accounts that are deeply privileged, the system is exposed to compromise since credential theft attackers will try to obtain service accounts with high-levels of privileges across the Windows infrastructure.

Following the Windows principle of least privilege, Dispatcher Phoenix addresses these concerns and ensures a more secure environment by using Windows impersonation. This means that the Dispatcher Phoenix application takes on the user's identity after the user is authenticated, instead of running as an administrative service account with broad access to the entire system.

This implementation of user impersonation is a critical and vital differentiating feature of the application, setting it apart from other application solutions in the marketplace today. Impersonation, known as one of the most useful mechanisms in Windows security, allows Dispatcher Phoenix to avoid granting one account unlimited access to folders, which can open up major security vulnerabilities throughout the system. For example, in Dispatcher Phoenix, folders are accessed as the logged-in user, not as an administrative service account that has read/write access to all network folders. By impersonating the Active Directory user, Dispatcher Phoenix ensures that ONE user does not have access to ALL folders.

Security Features

Dispatcher Phoenix provides a variety of security features that can be used to protect documents, including secure PDFs, intelligent redaction, automatic file deletion, and specialized processes to prevent illegal copying.

Password Protected PDFs

You can add passwords to PDFs to restrict users from opening, printing, and editing PDF documents. Once the document is processed through the secure Convert to PDF process, only those users who enter the correct password can open, edit, or print the document.

Redaction

With Dispatcher Phoenix's intelligent redaction technology, sensitive information can be permanently removed from electronic files. You can enter one or more search items to redact, choose the format of the output file, and specify where/how often the text should be redacted. Redaction can be set up as an automated process, or customized directly at the MFP panel.

Automatic File Deletion

Once files have been processed and sent to either local or network folders, Dispatcher Phoenix can automatically delete them after a set number of days.

Network

Konica Minolta MFPs are compatible with SNMP v1, 2, and 3. With more and more businesses choosing to disable SNMP v1 to tighten security, Dispatcher Phoenix is fully usable in environments where SNMP v1 is disabled. Dispatcher Phoenix can discover devices using SNMP v3, regardless of what type of encryption and authentication the site uses for SNMP. Alternatively, SNMP is not necessary at all if the site administrator supplies Dispatcher Phoenix with a list of MFP IP addresses.

Copy Defender

Dispatcher Phoenix's Copy Defender process protects documents from illegal copying by automatically applying the following customizable security features on printed documents:

- Copy Protect - Prints a copy security background pattern in the document. Text such as "Invalid Copy" or "Unauthorized" appears when the document is improperly copied. As an option, you can also add the date/time, distribution control number, serial number, and job number to the text, if needed. By printing text such as "Copy" or "Private" as a visible stamp, unauthorized copying is deterred.

- Stamp Repeat - Adds stamps such as "Copy" and "Private on the entire page.

- Copy Guard – Embeds a copy restriction pattern on all printed sheets. If an attempt is made to copy a Copy Guard sheet on a device that supports this function, the copying process is canceled and the job is deleted.

- Password Copy - Embeds a password on all printed sheets. If an attempt is made to copy a Password Copy sheet on a device that supports this function, the entry of a password is requested. Copying starts only if the correct password is entered.

Rx Shield

To help hospitals and clinics comply with federal mandates for secure prescription printing, Rx Shield automatically applies the following security features to printed prescriptions:

- Customizable Security Features Listing box to the bottom of the prescription.

- Copy security background pattern. Text such as "Invalid Copy" or "Unauthorized" appears when the prescription is improperly copied. As an option, you can also add the date/time, distribution control number, serial number, and job number to the text, if needed. Unauthorized copying is deterred when security warning text, such as "Copy" or "Private," appears as a visible stamp on the copied prescription.

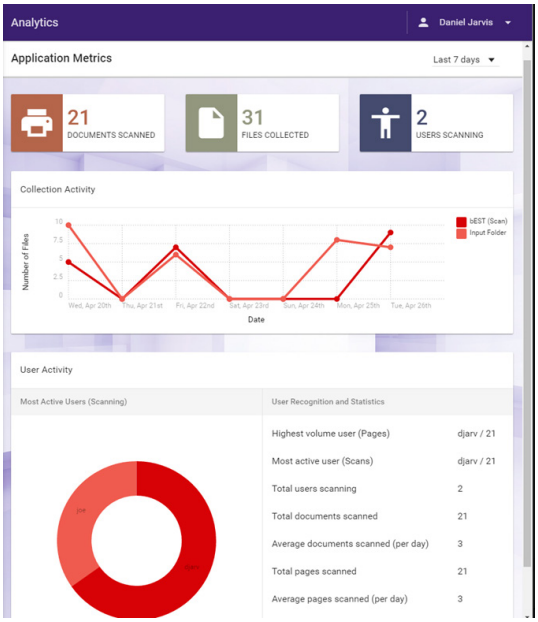
Auditing

Activity log files are recorded each day individually for each workflow, and Dispatcher Phoenix comes with a standalone Log Viewer that allows you to easily navigate through the workflow's history.

Dispatcher Phoenix also includes a workflow auditing feature that, when enabled, records/tracks important information about workflows. Some of the information is displayed on Dispatcher Phoenix Web's analytical dashboard, which displays metrics on:

- Number of document scanned
- Number of files collected
- Number of users scanning
- Metrics on collection activity
- Metrics on user scan activity
- Metrics on user recognition and statistics, such as:
    - Highest volume users
    - Most active user
    - Total users scanning
    - Total documents scanned
    - Average documents scanned

In addition, tracking data can be stored in a SQL database. Having this full audit trail of scans provides companies with the tools they need to take measures against.



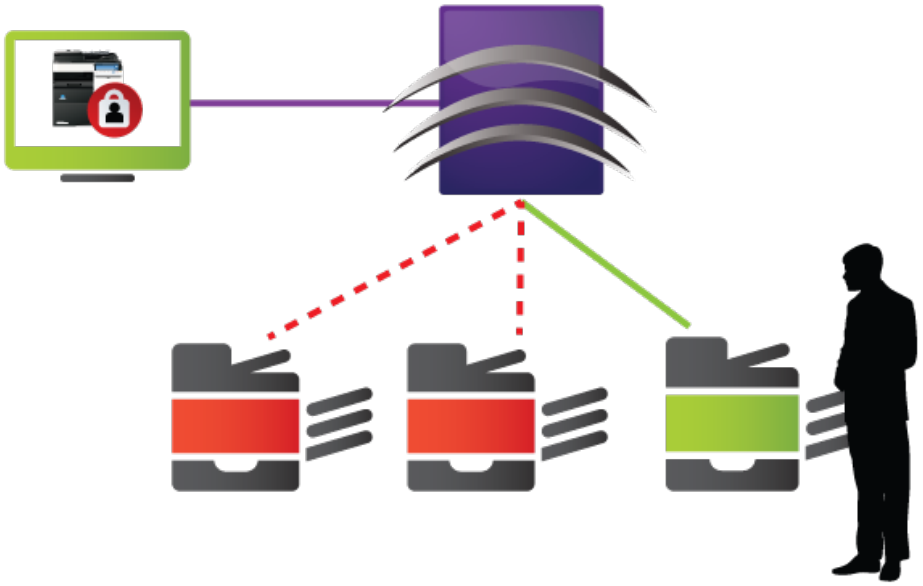
Secure Printing

Release2Me

One of the largest security threats today is the unrestricted access to documents that are often printed and left unclaimed in the output tray. If these unclaimed documents contain sensitive or confidential information, a major security risk is created. Our customers need a secure printing environment where they can control access to confidential documents at the printer. The ability to securely print out documents and eliminate the possibility of confidential information left exposed on printers is a key requirement in security-oriented companies and organizations.

Release2Me is Dispatcher Phoenix's secure print release system, which provides staff, managers, administrators, and other employees the ability to control confidential information. With Release2Me, print jobs are held in a queue until they are released at the MFP by an authenticated user. This ensures that documents are not printed until users enter a password or use an ID card to authenticate themselves at the MFP, confirming that they are physically present to pick up their printed documents. Since the print jobs are held in the queue on the server, not on the MFP's Hard Drive, the user can print these documents from any networked device. And unclaimed documents can be deleted from the queue after a user-specified amount of time.

Release2Me also works with the Dispatcher Phoenix Mobile app so mobile workers can release prints from their smart phones or tablets.



Document Encryption

When in transit from the MFP, data requires constant protection. Devices should be configured to use secure, encrypted network connections, especially when sensitive data such as documents and passwords may be transmitted. The MFP should encrypt data (both in Motion and at Rest) by SSL (Secure Sockets Layer) or TLS (Transport Layer Security). Dispatcher Phoenix supports the highest level of SSL/TSL that the device supports.

We also recommend that data on the MFP be secured with lock-down protection offered through bizhub SECURE, a set of enhanced password and data security measures to give the MFP an extra level of security that offers:

- Hard Drive Encryption
- Hard Drive Lock Password
- Automatic Deletion of Temporary Image Data
- Data Overwrite of Electronic Documents on a Timed Basis

Just as it is necessary to protect documents coming from the MFP into Dispatcher Phoenix, it is also important to ensure that processed documents are then stored securely. Dispatcher Phoenix provides a variety of connectors to document management systems, such as SharePoint and OnBase. We recommend that these systems enable powerful TLS encryption to protect data while it's being transferred between servers.

Default Access Ports

The following default access ports are used by Dispatcher Phoenix:

bEST	50808, 50809 (SSL)
FTP	21
KMBS MFP	59158, 59159 (SSL)
Printer (LPR)	515
Printer (RAW)	9100
SMTP	25, 465 (SSL)
SEC Workflow Worker Process	Needs Outbound access based on configured workflow (e.g., 53, 80, 443, 25, 445, 465, 587)
Add-In Manager	Outbound 80 (HTTP), 443 (HTTPS)
High Availability Set Up	• 4369 - Used by Heartbeat to define what each server's port is • 9000-9115 - Heartbeat negotiation range (range of servers' configurable ports)

Firewall Exceptions

When enabled, the Windows Firewall blocks all incoming network traffic to your computer except those applications and ports you allow. When installing Dispatcher Phoenix, please note that the following folders should be excluded:

- C:\Program Files\Konica Minolta\
- C:\Program Files (x86)\Konica Minolta\
- C:\Program Data\Konica Minolta

In addition, the following Dispatcher Phoenix executables most often trigger an alert:

- C:\Program Files\Konica Minolta\blox\blox-xmpp-cluster.exe
- C:\Program Files\Konica Minolta\blox\blox-xmpp-worker.exe
- C:\Program Files\Konica Minolta\conopsd\erts-5.10.4\bin\erl.exe
- C:\Program Files\Konica Minolta\conopsd\erts-5.10.4\bin\erlsrv.exe

Dispatcher Phoenix

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446

CountOnKonicaMinolta.com

12/15/2022