

# Securing Multifunction Digital Copiers

## Executive Summary

Multifunction products are digital copiers often equipped with printing, scanning and even fax capabilities. They are complex network devices that require careful security consideration when choosing the technology that you place in your office.

The recent CBS News report exposing the security risk of MFPs illustrated how manufacturers like Sharp, Toshiba, Xerox, HP, Canon, Ricoh, Savin, Lanier, and Konica Minolta, store a copy of each image the machine copies, prints, scans, or possibly even faxes on the hard drive.

If you did not see the CBS report you may view it on YouTube at this URL:  
<http://www.youtube.com/watch?v=D8vmXarBURo>

The CBS Report clearly showed the need for security, but the additional cost associated with security should be made at the time of acquisition and applied throughout the life of the equipment. Simply planning to remove the hard drive is not a reliable option. The hard drive must be intact to return a machine to a leasing company. Even if you pay cash for the machine, the hard drive could fail during your period of ownership and must be removed and replaced to restore functionality.

As pointed out in the report, the typical cost to add security to your device is \$500.00. This is a small price to pay for compliance with so many state and federal regulations concerning privacy, but it is still a bitter pill to swallow.

This white paper is for the non-technical executive level manager. The intention is to address issues of securing access to multifunction products (MFPs) and securing the information they produce. Any device that is placed on a network must be evaluated with respect to security.

## Secure Device Management

To practically manage a fleet of networked MFPs remote management is a must; however

the remote management must be secure. The device must allow authorized people to configure it while rejecting those that are unauthorized. Also, the process of managing the device must be secured so that the network traffic associated with the remote management cannot be sniffed, stolen or abused. How does the device protect itself from unauthorized access?

## Device Vulnerability

Does the device expose the network to any form of vulnerability? What sort of information does the device process and what are the security considerations related to that data? Networked MFPs operate independently on networks and can be a focal point for sensitive information. Securing them is in some ways comparable to securing other conventional networked devices such as computers. The need for controlled network access and the need for secure remote management are largely the same for MFPs and workstations.

In other areas, the security considerations around MFPs are substantially different. MFPs generally don't run conventional operating systems, the concept of user authentication is applied differently, they do not have network file shares that need to be secured and they probably do not need or support antivirus software.

## Administrative Access and Passwords

The ability to change the device settings must be controlled using device passwords. This keeps unauthorized users from altering the device's settings, including security settings. The device administrator must provide one of these passwords to be granted permission to configure the device through its web interface and management tool.

There should be no support for creating additional passwords, and no means to grant administrative access to users or administrative accounts that exist in the corporate domain,

# Securing Multifunction Digital Copiers

outside of the MFP. The Advanced Password allows an administrator to configure the MFPs settings, but should not give access to the MFPs operating system or hard drive. The operating system and the device's file system must be secure and not exposed to external configuration, by any means. Passwords must protect the configuration of the device via the touch screen operator panel and through network access via HTTP, HTTPS, and telnet.

## Using HTTPS

The benefits of using HTTPS to access the device's web interface include:

- Ease of use in establishing the connection for the end user. The browser just needs to be pointed to "https://" instead of "http://". The rest should be automatically taken care of by the MFP and the browser.
- Encryption of all data exchanged through the browser – this includes the MFPs passwords, and any other settings that are set or viewed.
- Support by most commonly used web browsers – HTTPS and SSL are extremely prolific standards.
- Integration into pre-existing certificate authority (CA) – the MFPs certificate that allows the SSL session to be established can be signed by a certificate authority.

## SNMPv3

SNMP (Simple Network Management Protocol) provides another means to remotely configure MFPs. It can be used to view and alter MFP settings, so it involves the basic security questions of how to control its use and how to protect the associated network traffic when it is used. This standard protocol includes support for authentication and for data encryption.

Authentication allows authorized systems to see and manage the MFP via SNMPv3, while shutting out unauthorized systems. Encryption of the SNMPv3 packets protects the information from being sniffed by the network, or, more accurately, the sniffed data is useless because it is encrypted.

## IP Security (IPSec)

IPSec (IP Security) is an extremely important mechanism, since it allows the MFP to establish a secure connection to other network nodes such as print servers and management workstations.

IPSec is available on conventional operating systems (Windows, Linux, etc.), and by applying IPSec between the MFP and a workstation or server the traffic between these systems can be secured with strong encryption.

IPSec provides many benefits, including:

- Encryption of scanned jobs on the network including images scanned to FTP, email, or any other network destinations.
- Encryption of print jobs on the network, and decryption by the MFP.
- Remote configuration (by a web session, telnet, SNMP, or any other IP-based means) can be secured. Since mechanisms like HTTPS and SNMPv3 can provide security, as described above, this can be a redundant level of security. Alternately, IPSec can be relied upon to provide the security, simplifying the other mechanisms.

## 802.1x Support

In almost all network environments, users are required to log on to the network before they can do things such as send or receive email, browse the web, etc. This can be taken to another level where devices such as laptops or MFPs can be required to authenticate before they are allowed on the network. The protocol for performing this authentication is 802.1x.

802.1x allows the MFP to authenticate itself on the network, increasing security. With support for a wide array of authentication methods, the 802.1x authentication mechanism will be compatible with almost any 802.1x authentication environment. 802.1x is compatible with wireless network adapters, which provides secure wireless networking capabilities.

# Securing Multifunction Digital Copiers

## Device Hardening

Hardening a networked device is the process of securing the device's network interfaces. This includes eliminating unneeded or unused features and functions to prevent their abuse, locking down any interfaces that remain, and securing the data hosted by the device.

## Port Filtering

Port filtering allows the MFP to be configured to comply with virtually any policy in regards to which protocols are and are not allowed on the network.

The benefits include:

- Increased security by granular and authoritative control over the protocols the device processes, or ignores.
- Cleaner port scans – shut down the unneeded ports, and ports scans will not report “phantom” vulnerabilities that need to be tracked down and understood.
- Redundancy – many protocols (such as HTTP, FTP, DHCP and others) can be disabled on the MFP, and port filtering allows the corresponding ports to be disabled as well.
- Reduced network traffic.

## Hard Drive Encryption

A common concern for networked devices is that data will be exposed to remote access on the network. For example, what if a system has appropriate protections for data while it is in use, but not when the data is idle? Does leftover data remain on a system, and if so, is it less well protected than it should be?

MFPs use hard drives for a variety of purposes, including buffering scanned data during the course of copy jobs and buffering print data during print jobs. It is important to ensure the buffered data is well protected, so no one can access potentially sensitive information contained in scan or print jobs the MFP receives.

Hard drive encryption protects not only residual data left over after jobs, but also protects data actively being used. This prohibits someone

from powering off the MFP in the middle of a job and making use of data abruptly left on the drive.

## Hard Drive Wiping

When a data file is “deleted” from a hard drive, the data that is associated with that file is not actually deleted. This data remains on the hard drive and could, as shown in the CBS News Report, can be recovered.

Hard drive wiping actively overwrites the entire hard drive with multiple passes of data, removing all residue of prior information.

## TCP Connection Filtering

TCP connection filtering through the “Restricted Server List” feature allows the MFP to accept only previously specified TCP/IP connections and reject all others.

Specifying a Restricted Server List would allow:

- Approved systems such as print servers and administrative workstations are allowed to make connections to the MFP, so normal and approved functions such as printing and routine monitoring and maintenance occur normally.
- All network interactions that involve TCP/IP connections to be controlled to increase security.

The types of connections that rely on TCP/IP include HTTP/browser connections, FTP, telnet and printing via LPR/LPD or through the Windows print subsystem.

- Unknown systems would be left off of the list, which secures the MFP against unauthorized external connections.

## Separation of Fax and Network Traffic

A common question about networked MFPs is whether there's an exposure created by the presence of a fax modem. The concern is that one could “dial up” the MFP via the fax modem and manipulate the device, or somehow gain access to the network to which the MFP is connected.

In fact, some manufacturers have designed software to allow them access to the MFP via the phone line. This access was designed to

# Securing Multifunction Digital Copiers

allow the service department to gather data about the machine, upgrade firmware, and clear error codes. The manufacturer of your specific model machine would have to address the existence of such software to access your equipment. The exposure of retrieving facsimile images is the primary risk and of course the topic of this paper.

## Digitally Signed Firmware Updates

MFPs should only support a firmware download process by which the firmware that controls all of the device's behavior can only be updated using digitally signed firmware updates from the manufacturer. This is an appropriate feature, used to add new features and correct problems when necessary.

It's important that these firmware updates are carefully controlled, to avoid any exposure to unauthorized code being placed on the device.

## Confidential Print

Confidential Print is a feature that addresses the basic concern of printed pages lying on the MFP for anyone to pick up. With Confidential Print, the MFP holds submitted jobs until the intended recipient is present at the device. By producing the printed job only when the proper PIN code is entered on the MFP's operator panel, the job is delivered securely into the right hands.

When a hard drive is present, jobs are retained across power cycles of the MFP, and the number of jobs that can be held by the MFP is greatly increased. Jobs stored on the MFP's hard drive leverage the security of Hard Disk Encryption. Jobs stored in this way cannot be moved to a different MFP or pulled off the hard drive.

## User Authentication

Some secure environments will need the user that approaches the MFP and selects a function, such as Scan-to-Email, to authenticate (i.e. "log on") before proceeding. This limits the function access to valid users only, and allows

the MFP to identify the user performing the function.

User Authentication provides security features that include:

- Securing the MFP by limiting who can use its "walk up" functions.
- Anonymous e-mail is avoided by inserting the identity of the authenticated user into the email generated with the scan-to-email function.
- When users authenticate, they should use their normal login and password, just as if logging onto their workstation or laptop. This keeps the process simple and intuitive.
- Faxes sent via networked fax servers can automatically send an email confirmation of the fax to the sender's email, since the MFP "knows" who is sending the fax.
- The companies to which e-mail is sent can be limited to a predetermined destination (for example, @company.com), so that e-mail can't be sent to arbitrary destinations.

## Address Book Lookup via LDAP over SSL

When performing a Scan to Email or Scan to Fax operation, users can look up the recipient's email address or fax number, rather than having to know the information and type it all in. This important convenience feature is made possible through LDAP. LDAP allows the MFP to query the corporate directory for information. The use of SSL adds security to the process. By establishing an SSL connection before generating LDAP queries, the MFP and the directory server protect the information they exchange.

## MFP Lockout

The MFP Lockout feature allows an MFP to be put in a locked state where the operator panel doesn't allow any user operations or configuration, and incoming print jobs are stored on the MFP's hard drive instead of being printed. This secures an MFP during off hours: it cannot copy or scan jobs. It cannot be reconfigured via the operator panel, and incoming jobs will not sit exposed in the output bin. When the time is right, the MFP can be unlocked by entering a preconfigured PIN, at

# Securing Multifunction Digital Copiers

which time the held jobs will be printed and the MFP resumes its normal operation.

MFP Lockout provides for an easily secured MFP during off hours, with scanning and printing operations disallowed. Jobs printed to a locked MFP cannot be stolen from the output bin. This would complicate after hours theft of confidential documents.

## USB Device Restrictions

If enhanced security is required, an MFP should have the ability to limit or disallow USB functions including:

- Disallowing users to perform scan-to-USB operations in environments where sensitive documents must be carefully controlled.
- Disallowing users to perform print-from-USB operations in environments where printing is tracked or allowed only on a fee-basis.

- Limiting the ability to perform scan-to or print from USB devices to only authenticated users for additional security.

## Summary

MFP security is about protecting the MFPs, the network, and the data that's involved in the use of the MFPs. MFP security is a complex issue, with many elements to consider. Speak with your Clear Imaging Solutions representative to discuss how we achieve your security benefits with a major manufacturer of MFPs that has a long legacy of data security built into their devices and there is no extra cost for security and peace of mind.