technical white paper

LEXMARK

> Security and Lexmark Multifunction Products: Overview of Features

Rich Russell, Technical Security Consultant

February, 2006

Contents

Executive Summary

Multifunction products, or MFP's, are complex network devices that require careful security consideration. Lexmark MFP's and networking products include a wide array of security features. This document discusses the security features of Lexmark MFP's and provides an overview of their benefits and their implementation.

Any device that is placed on a network must be evaluated with respect to security. How does the device protect itself from unauthorized access? 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? These, and many other questions, are appropriate to ask of any networked device, including networked MFP's.

Networked MFP's 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 MFP's and workstations. In other areas, the security considerations around MFP's are substantially different. MFP's 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.

This document will define the major areas of security concerns related to MFP's and provide an overview of the security features of Lexmark MFP's that allow the devices to be deployed, managed and used in a secure manner.

Applicability

This white paper applies to the following Lexmark products:

- Lexmark X644e MFP
- Lexmark X646dte MFP
- Lexmark X850e MFP
- Lexmark X852e MFP
- Lexmark X854e MFP

This white paper does not constitute a specification or warranty. All rights and remedies concerning products are set forth in each product's Statement of Limited Warranty.

Secure Device Management

To practically manage a fleet of networked MFP's 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.

Lexmark MFP's include a variety of features to make remote device management easier, and more secure.

Administrative Access and Passwords

Overview

The ability to change the device settings can be controlled using device passwords. This keeps unauthorized users from altering the device's settings, including security settings.

Lexmark MFP's support two passwords; this allows two levels of access and control to be established. The device administrator must provide one of these passwords to be granted permission to configure the device.

When an attempt is made to configure the MFP via the web browser, the appropriate password must be provided. The "User name" is not required.

This control applies to network access via the device's web server, as well as to configuration of the MFP through its touch screen operator panel.

Benefits

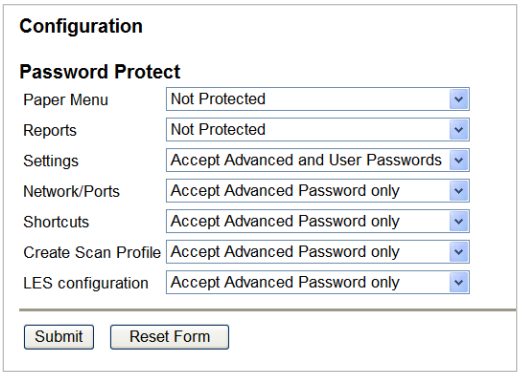
Support for administrative passwords is a basic building block of security; it allows the device to be protected against unauthorized configuration while allowing authorized administrators to configure the device.

Support for two levels of administrator provides granularity. The MFP can be configured to allow a limited set of control for one or more users while reserving control over the device's most sensitive settings for authorized administrators.

Details

The device supports two administrative passwords. The "Advanced Password" provides control over all of the MFP's settings, while the "User Password" allows configurable access.[1]

The device settings can be unprotected, limited to users and administrators, or restricted to administrators only.



In this example the Paper settings and the ability to print Reports is exposed without the need to provide a password. The ability to change the basic device Settings is available only to those that can provide the User or Advanced password. All other settings are restricted to administrators who can provide the Advanced password.

The passwords must be at least 8 characters in length, and can be up to 128 characters in length. Passwords can include alphabetic, numeric, and other characters to allow for substantial complexity. There is no support for creating additional passwords, and there are no means to grant administrative access to users or administrative accounts that exist in the corporate domain, outside of the MFP.

The Advanced Password allows an administrator to configure the MFP's settings, but does not give access to the MFP's operating system or hard drive. The operating system and the device's file system are not exposed for external configuration, by any means.

The passwords protect the configuration of the device via the touch screen operator panel and through network access via HTTP, HTTPS, and telnet.

HTTPS

Overview

The most common means to remotely configure most network devices, including MFP's, is through the device's web interface. Point a browser to the MFP's IP address or DNS name, and if you can provide the MFP's password (as described above in Administrative Access and Passwords) you can configure the device's settings.

However, browsers and the HTTP traffic associated with them are not inherently secure. Someone could sniff the network traffic used in the web session and determine the device's password. To address this concern, Lexmark MFP's support HTTPS.

Benefits

The benefits of using HTTPS for web sessions 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 is automatically taken care of by the MFP and the browser.
- Encryption of all data exchanged through the browser – this includes the MFP's 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) or PKI environments – the MFP's certificate that allows the SSL session to be established can be signed by a certificate authority.

[1] The User Password is not associated with user accounts in the corporate directory. Like the Advanced Password, it is a password that is stored only on the MFP. Settings that users should be able to modify can be associated with this password (per the illustration, above), and the password should be shared with those users who are authorized to modify the corresponding device settings.

With HTTPS, web sessions can be conveniently and effectively secured.

Details
The MFP includes an embedded web server, and when a browser is pointed to the MFP's address with the "https://" prefix the MFP and the client system negotiate an SSL connection. This involves the MFP passing its x.509 certificate to the client system, to establish its (the MFP's) identity. Since the MFP's certificate is self-signed by default, the client will typically present a warning to the user (whether and how this happens depends on the settings of the web browser). The client system can choose to trust the self-signed certificate, and thereafter receive no further warnings.

Alternatively, the MFP's certificate can be signed by a CA. This can be an external CA or a CA that is internal to the customer's environment. The MFP's web interface includes a Certificate Management page that facilitates this process.

Replacing the self-signed certificate with a CA-signed certificate avoids the warnings associated with HTTPS sessions.

The HTTPS session is built on an SSL connection in which all exchanged data is encrypted. This protects the contents of the session against eavesdropping, and allows for secure remote management of the printer.

SNMPv3

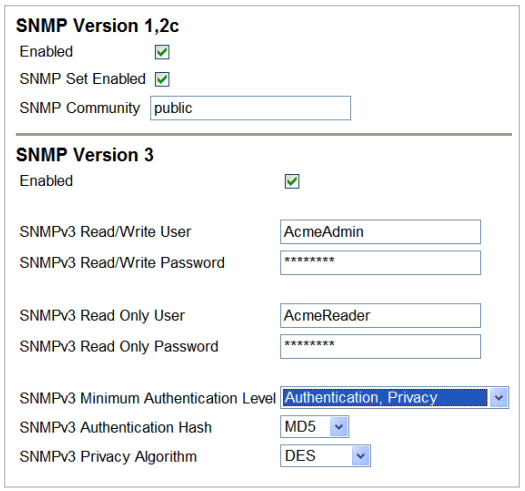
Overview
SNMP (Simple Network Management Protocol) provides another means to remotely configure MFP's. It can be used to view and alter MFP settings, so it involves the basic security questions of how to control its use and how to protect the associated network traffic when it is used.
Lexmark MFP's support the latest version of SNMP (SNMPv3), and SNMPv1 and v2 for backwards compatibility. This standard protocol includes support for authentication and for data encryption.

Benefits
Support for SNMPv3 allows Lexmark MFP's to be managed securely by standard SNMP console applications. There are two important elements to the security provided by SNMPv3:

- 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.

Details
The authentication features of SNMPv3 allow the MFP to refute SNMPv3 traffic unless the requests are preceded by an authentication (via MD5 or SHA1). The MFP supports two SNMPv3 accounts. Authenticating against one yields the ability to read the MFP's settings but not write them; authenticating against the other provides the right to read and write the MFP's settings.

Support for data privacy in SNMPv3 means that the MFP and SNMP client can use an encryption algorithm (DES, or AES with 128, 192, or 256 bit keys) to encrypt the SNMPv3 traffic.



SNMP v1 and SNMPv2 can be enabled or disabled independently of SNMPv3. And, SNMPv3 supports both authentication and privacy features.

As with other mechanisms for managing the MFP, SNMP can be disabled – if it is not used in a particular environment it can, and should be, turned off entirely.

IP Security (IPSec)

Overview
IPSec (IP Security) is supported on Lexmark MFP's. This 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.

Benefits
IPSec can provide 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 their own 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.
- Protection of all traffic between Lexmark's management application, MarkVision Professional (MVP), and the MFP.

In short, IPSec can be used to protect virtually any form of IP-based network traffic between the MFP and a set of hosts, no matter what operation is performed by that traffic.

Details
Lexmark MFP's support IPSec with pre-shared keys and with certificates.

In pre-shared key mode, the MFP can be configured to establish a secure IPSec connection with up to five other systems. The MFP and these systems are configured with a passphrase, which is used to authenticate the systems and to encrypt the data subsequently.

In certificate mode, the MFP can be configured to establish a secure IPSec connection to up to five other systems or subnets. This allows the MFP to exchange data securely with a large number of systems, and the use of certificates allows the process to be integrated with a PKI or CA infrastructure. This provides a more robust and scalable solution, without the burden of configuring or managing keys or passphrases.

The MFP can store and apply two certificates, for use with IPSec. The MFP includes a self-signed certificate that can be replaced with a certificate signed by a CA. This certificate can be generated from scratch, or it can be generated with the base64 encoded PKCS file that's embedded in the MFP and available through its web interface. This allows the MFP's identity to be validated by other systems in the CA environment. In addition, the MFP can store the CA's certificate as a trusted root CA certificate, allowing it to validate the identity of other systems in the CA environment.

IPSec can be used in preshared key mode and certificates mode, simultaneously.

802.1x Support

Overview
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 MFP's can be required to authenticate before they are allowed on the network. The protocol for performing this authentication is 802.1x. Lexmark MFP's support the 802.1x protocol for device authentication.

Benefits
802.1x provides the following benefits:

- It 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 the optional wireless network adapter, which provides secure wireless networking capabilities.

Details
Typically, 802.1x support is only leveraged for wireless devices. Most environments only support or require 802.1x authentication for network edge devices and for wireless connectivity. Lexmark's implementation of 802.1x supports both wired and wireless environments.

Lexmark's 802.1x supports the following network authentication methods:

- LEAP
- PEAP
- EAP-MD5
- EAP_MSCHAPV2
- EAP-TLS
- EAP-TTLS with the following authentication methods:
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - PAP

The MFP supports all of these protocols and can be configured to include or exclude each protocol in the 802.1x protocol negotiation.

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.

Lexmark MFP's include a variety of mechanisms to facilitate in the device hardening process.

Port Filtering

Overview
Port filtering is implemented on Lexmark MFP's as a granular filter that allows network ports to be individually disabled. This 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.

Benefits
Support for filtering individual ports provides a variety of benefits, including:

- 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.

Details
The MFP allows each of twenty five TCP and UDP ports to be individually opened or closed:

TCP 21 (FTP)	UDP 5353 (MDNS)
UDP 68 (DHCP)	TCP 8000 (HTTP)
UDP 69 (TFTP)	TCP 9000 (Telnet)
TCP 79 (FINGER)	TCP 9100 (Raw Print)
TCP 80 (HTTP)	UDP 9100 (HBN3)
TCP 443 (HTTPS)	TCP 9200 (IR Alerts)
UDP 137 (WINS)	UDP 9200 (Discovery)
UDP 161 (SNMP)	UDP 9300 (NPAP)
UDP 162 (SNMP Traps)	TCP 9400 (Lexmark
TCP 515 (LPR/LPD)	Print Port)
TCP 631 (IPP)	TCP 9500 (NPAP)
UDP 1584 (HBN1)	TCP 9600 (IPDS)
TCP 5000 (XML)	UDP 9700 (Plug-n-Print)
TCP 5001 (IPDS)	TCP 10000 (Telnet)

Each port can be opened or closed. When closed, the MFP will not generate or respond to traffic on the specified port even if the corresponding network application is otherwise enabled or disabled.

Hard Drive Encryption

Overview
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?

MFP's 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.

Lexmark MFP's can encrypt all data on their hard drives to protect it from external access at all times.

When this feature is enabled, all data written to the hard drive is encrypted. This 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.

Benefits
The benefits of hard drive encryption include:

- Increased security of active and residual data.
- The hardware-assisted encryption is applied in real time, so there is no delay for cleanup or post-processing after jobs have completed.
- A dynamically-generated encryption key stored on the MFP (not the hard drive) makes the data on an encrypted drive useless on any other MFP. Stealing the hard drive out of the MFP will not yield access to the data it contains.[2]

Details
By default, the data on the MFP's hard drive is notencrypted. This does not mean the contents of the drive are exposed. There is no path by which residual job data can be retrieved or accessed remotely.[3]

When hard drive encryption is activated, the encryption key to be used (128 bit AES symmetric encryption) is pseudo-randomly generated and stored in a proprietary fashion in the MFP's memory. Note that the key is not stored on the hard drive itself, so if the hard drive were stolen from the MFP the contents of the drive would remain indecipherable.

When the encryption function is activated, the hard drive is formatted and all data contained on the drive is lost. The encryption is then applied to all data placed on the hard drive, at all times.

Hard Drive Wiping

Overview
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, with substantial efforts, theoretically be recovered.

Lexmark MFP's support an additional mechanism for protecting residual data: hard drive wiping. Hard drive wiping actively overwrites the entire hard drive with multiple passes of data, removing all residue of prior information.

Benefits
The benefits of hard drive wiping include:

- Increased security of residual data.
- Elimination of the need to remove or process the hard drive when the device is to be retired, recycled, or otherwise removed from a customer's secure environment.

Details
The MFP's hard drive is used exclusively for buffering data: scanned data, incoming print jobs, and any other image data related to jobs being processed by the MFP. The wiping process applies to the entire hard drive, so all residual data left over from buffered print or scan data is addressed in the process.
The hard drive wiping process can be activated manually, through the MFP's operator panel.

TCP Connection Filtering

Overview
Lexmark MFP's support TCP connection filtering through the "Restricted Server List" feature. This feature allows the MFP to accept only previously specified TCP/IP connections and reject all others.

Benefits
Specifying a Restricted Server List includes the following benefits:

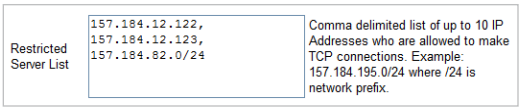
- Approved systems such as print servers and administrative workstations are allowed to make connections to the MFP, so normal and approved functions such as printing and routine monitoring and maintenance occur normally.
- All network interactions that involve TCP/IP connections can be controlled to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

[2] Note that this doesn't render the hard drive, itself, useless: when an encrypted hard drive is moved from one MFP to another, it must be reformatted when it's placed into the new MFP. The drive is portable, but the data on it is not.

[3] There are lots of factors that lead to this—more than are pertinent for this white paper. Briefly: there's no means by which to have the MFP reprint or retrieve residual data, the MFP doesn't support a network file system or file sharing, and there's no protocol supported by the MFP that allows one to arbitrarily read or write data from the hard drive. So even without encryption of the hard drive's data, the disk drive contents are well protected.

print subsystem. All of these connections will be allowed only to/from the specified systems.
- End-user systems can be left off the list, which prohibits them from connecting to the MFP via avenues such as a web browser or FTP connection.
- Unknown systems would be left off of the list, which secures the MFP against unauthorized external connections.

Details
The Restricted Server List allows up to 10 IP addresses or subnets to be specified. The MFP responds normally to any address in the list, and rejects TCP connections to any address that's not in the list.



The Restricted Server List allows individual addresses and subnets to be specified. TCP connections from all other addresses will be refused by the MFP.

The Restricted Server List does not affect UDP traffic, so connectionless interactions (such as a ping) are allowed from any address.

Separation of Fax and Network Traffic

Overview
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, there's no exposure of this sort on Lexmark's MFPs. The fax modem allows for the exchange of facsimile images, only. There's no path by which the fax modem connection can interact with or control the MFP's network interface, and there's no facility for configuring the MFP's settings via the fax modem connection.

Said simply, the fax modem connection allows one to send and receive fax images, and nothing more.

Benefits
Support for fax on a networked MFP includes the following benefits:

- Incoming fax images can be printed as hard-copy documents, or routed to a predefined email, FTP, or workflow destination. Note that this does not undermine the network's security in any way, since the incoming data can only be in an image format. The fax connection cannot receive or transmit executable data such as applications, scripts, or viruses.
- Incoming faxes can be redirected to an alternate fax machine. This could be used when an office is temporarily closed, to allow incoming faxes to be forwarded to an alternate device that's being regularly monitored.

Details
The fax modem connection is restricted to Facsimile Class 1 mode, and the data transferred over the modem is limited to facsimile image data, only. The connection is not like a laptop modem or other device where an arbitrary network connection can be established via the fax modem. The information exchanged over the MFPs modem is restricted to image data, only.

Network protocols are not supported through the fax modem. There's no support for exchanging TCP/IP traffic of any sort, including telnet, FTP, HTTP, SNMP, or any other form of network packet.

There's no support for modifying the MFP's configuration via the fax modem connection. Settings can't be viewed or changed, and there's no access to the MFP's file system through the fax connection.

Digitally Signed Firmware Updates

Overview
Lexmark's MFPs support a firmware download mechanism, by which the firmware that controls all of the device's behavior can be updated. This is a common and 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.

Lexmark's MFPs perform multiple checks on downloaded firmware before adopting the firmware or executing any code contained in the package. This prohibits one from placing unauthorized code of

any sort on the device, and inappropriately altering the MFP's behavior.

Benefits
The benefits of digitally signed firmware updates include:

- The MFP's capabilities can be maintained and extended through the application of appropriate and authorized firmware updates.
- Unauthorized firmware packages and applications cannot be added to the MFP. If the code was not built and signed by Lexmark, the MFP rejects and discards the package.

Details
Lexmark's MFP's and printers inspect all downloaded firmware packages for a number of required attributes before the firmware is adopted or executed. The firmware must be packaged appropriately, in a proprietary format. In addition, packages must be encrypted with a symmetric encryption algorithm with a key that's known only to Lexmark and embedded securely in all MFP's. But the strongest security comes from the requirement that all firmware packages must include multiple digital 2048-bit RSA signatures from Lexmark. If these signatures are not valid, or if the message digests that accompany them indicate that the firmware has been changed in any way since the signatures were applied at Lexmark, the firmware is discarded.

Firmware updates can be transmitted over the network, allowing the devices to be conveniently updated en masse. This process can be automated and scheduled, and the process does not require one to be present at the device. For security, the ability to perform this update over the network can be limited to authorized administrators. The MFP receives the code, validates it, adopts it, and restarts automatically. The process takes just a few minutes, and the MFP is available for use immediately afterwards.

Lexmark's MFP's support custom Java applications through an embedded application platform, and the Java applications must also be digitally signed by Lexmark before being adopted. This prohibits external users from placing unauthorized applications on Lexmark's MFP's, by any avenue.

Secure Device Operation

Lexmark MFP's include standard features to secure the use of the device, ensuring only appropriate users use the device functions and that the information associated with those users is protected.

Confidential Print

Overview
The Confidential Print feature 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.

Benefits
The features and benefits of Confidential Print include:

- An intuitive and effective means to deliver print jobs only when the recipient is at the MFP.
- Security is provided with 4-digit PIN's from 0000-9999—there are 10,000 possible values.
- The standard feature operates whether or not the MFP is equipped with an optional hard disk. If no hard disk is present, the print job is held in the MFP's RAM memory.
- If a hard disk is present, print jobs will be stored on the disk. This allows for more jobs to be held, and jobs will be retained if the MFP is powered off. If Hard Drive Encryption is enabled (see page 6), the stored jobs will be encrypted for additional security.
- Unprinted jobs can be automatically purged after a specified amount of time, to avoid buildup of old jobs.

Details
Lexmark MFP drivers can be directed to submit Confidential Print jobs by specifying a Confidential Print PIN (Personal Identification Number). This is a standard feature on Lexmark MFP drivers and MFP's.

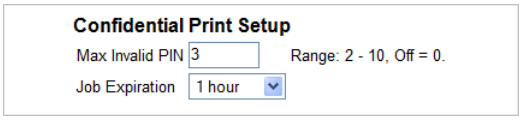
When the MFP receives a Confidential Print job, the data stream is stored on the MFP's RAM memory or

on the MFP's hard disk if the hard disk option is present. Jobs stored in the MFP's RAM memory will be deleted if the MFP is powered off, and can be deleted automatically by the MFP if a memory shortage is encountered. For these reasons, it's strongly recommended that a hard disk be installed if Confidential Print is to be used extensively.

When a hard disk 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 disk leverage the security of Hard Disk Encryption. Jobs stored in this way cannot be moved to a different MFP on the hard disk. As discussed on page 7, encrypted hard drives cannot be moved from one MFP to another without being reformatted.

For additional security, setting a maximum number of retries on PINs prevents brute-force attempts to guess PINs. If the PIN is entered incorrectly the specified number of times, the corresponding print job(s) will be deleted.



Setting a maximum number of invalid PIN entries thwarts attempts to guess PINs, and jobs can be set to expire after a range from one hour to one week.

And, the Job Expiration feature allows jobs to be automatically deleted from the MFP after a specified time interval, ranging from one hour to one week.

User Authentication

Overview

When a user approaches the MFP and selects a function such as Scan-to-Email, the MFP can require the user to authenticate (i.e. "log on") before proceeding. This limits the function access to valid users, and allows the MFP to identify the user performing the function.

An important aspect of User Authentication is allowing the user to enter their "normal" user ID and password. The user should not, and does not, have to remember a special set of information to use the MFP. Instead, the MFP should, and does, make use of the corporate directory to validate users' credentials against the standard, centralized database.

Benefits

The benefits of User Authentication 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 e-mail generated with the scan-to-email function.
- When users authenticate, they 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.

Details

The MFP can restrict access to the following functions:

- Copy
- Scan to Email
- Scan to Fax
- Scan to FTP
- Printing Held Jobs (such as Confidential Print jobs)
- The ability to print jobs from a USB "thumb drive"
- The ability to scan jobs to a USB "thumb drive"
- Launching Embedded Applications

Note that access to these functions can be set individually, and ranges can be set to any of the following levels:

- No Authentication Required –Wide open access, so that anyone can use the device without any authentication at all. This is appropriate when no control or tracking is necessary.
- Require User ID only – in this mode the user is required to indicate their User ID, but not their password. This is appropriate when users can be trusted to correctly identify themselves, and tightly-controlled access is not necessary.
- Require User ID and Password – this mode requires users to enter their valid User ID and

corresponding password before making use of the protected function.
- Function Disabled – each function can be disabled entirely, for environments where the given function is not needed or not appropriate. Disabled functions are not displayed on the MFP's touch screen operator panel.

The process of authenticating the user's credentials is flexible, as well. The MFP can use a variety of protocols to validate the user's information: LDAP, LDAP over SSL, Kerberos, or NTLM. Support for a wide array of authentication protocols means that the MFP's User Authentication function is compatible with a wide array of network environments, including Microsoft's Active Directory, Novell's eDirectory, as well as any other directory environment that supports LDAP.
The use of secure User Authentication protocols such as LDAP over SSL, Kerberos, and NTLM protects users' credentials during the authentication process.

Address Book Lookup via LDAP over SSL

Overview
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.

Benefits
The benefits of performing LDAP over SSL include:

- The information queried by the MFP is secured (encrypted) on the network.
- The MFP leverages a customer's existing PKI infrastructure to perform SSL, conforming to the customer's standard security practices

Details
The MFP can be configured to trust the customer's CA by installing the CA's X.509 certificate on the MFP. Multiple certificates can be installed, to establish trust to more than one CA.
When configured to do so, the MFP will precede all LDAP traffic with the negotiation of an SSL connection: the directory server will provide it's certificate, the MFP will validate it, and a secure (encrypted) communication channel will be established. All subsequent LDAP traffic will take place over this channel, so all LDAP information will be encrypted on the network. This applies to LDAP-based user authentication, as well as LDAP queries for email and fax information.

MFP Lockout

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

Benefits
The features and benefits of MFP Lockout include:

- 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.

Details
MFP Lockout is set up under administrative control, via the MFP's embedded web page. A 4-digit PIN is specified. That PIN can then be used to lock or unlock the MFP on its operator panel. This feature requires that an MFP hard disk be present.

When the MFP is locked, the operator panel does not allow any interaction other than specifying the PIN to unlock it. While locked, incoming print jobs and faxes are not printed, but stored on the MFP's hard disk. If Hard Disk Encryption is enabled, then jobs stored on the hard disk will be encrypted.

When the MFP is unlocked, jobs received during the locked period are printed. Any Confidential Print jobs received during the locked period are not printed, but are available through the typical Confidential Print jobs interface on the MFP's operator panel.

Note that this feature is available on models that include a hard disk: the X646e, X850e, X825e, and X854e MFP's. This feature is not available on the X644e MFP model.

USB Device Restrictions

Overview
Lexmark MFP's support USB "thumb drive" devices for printing and scanning. One can print image files (JPEG, TIFF, BMP, PDF) from thumb drives, and store scanned pages on thumb drives.

If enhanced security is required, the MFP has the ability to limit or disallow these operations.

Benefits
The benefits of restricting the functions of USB devices include:

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

Details
The MFP only allows USB devices such as "thumb drives" to be used for scan-to-USB or print-from-USB. Other operations from USB devices are disallowed. The MFP's configuration cannot be set or recorded, and the MFP's firmware can't be modified or updated from USB devices.

The ability to scan-to or print-from USB devices can be controlled separately, and set independently to any of the following states:

- Active, and No Authentication Required – The functions are active, and no authentication is required. This is appropriate for environments where no control or tracking is necessary.
- Require User ID only – in this mode the user is required to indicate their User ID (but not their password) prior to using the USB device. This is appropriate when the users can be trusted to correctly identify themselves, and tightly-controlled access is not necessary.
- Require User ID and Password – this mode requires users to enter their valid User ID and the corresponding password before making use of the protected USB function.
- Function Disabled – the MFP won't allow print-from and/or scan-to USB devices, at all.

Summary

MFP security is about protecting the MFP's, the network, and the data that's involved in the use of the MFP's. MFP security is a complex issue, with many elements to consider.

Lexmark MFP's are equipped with an array of security features that allow you to secure networked MFP devices and their use:

- Lexmark MFP's can be managed securely with device passwords, HTTPS, SNMPv3, and IPSec
- Lexmark MFP's can be hardened with Port Filtering, TCP Connection Filtering, Hard Drive Encryption, and Hard Drive Wiping
- Lexmark MFP's can by operated securely with Secure User Authentication, LDAP over SSL, Confidential Print, and MFP Lockout