

Security and Lexmark Multifunction Products: Overview of Features

This document will define the major topics of securing the Lexmark multifunction product (MFPs) and provide an overview of the security features and functionality of these devices. This will allow the devices to be deployed, managed, and used in a secure manner on your network.

Executive Summary.....	3
Applicability.....	3
Secure Device Management.....	4
Function Access Controls, Authentication/Authorization, and Backup Passwords.....	4
HTTPS.....	6
SNMPv3.....	8
IP Security (IPSec).....	9
802.1x Support.....	10
Device Hardening.....	11
Port Filtering.....	11
Hard Disk Encryption.....	12
Hard Disk Wiping.....	14
TCP Connection Filtering.....	14
Separation of Fax and Network Traffic.....	15
Digitally Signed Firmware Updates.....	16
Secure Device Operation.....	17
Confidential Print.....	17
User Authentication and Authorization.....	19
Address Book Lookup via LDAP over SSL.....	21
Operator Panel Lock.....	22
USB Device Restrictions.....	22
Summary.....	23

Executive Summary

Multifunction products, also referred to as MFPs in this document, can be complex network devices that require security considerations. Lexmark MFPs, as with other networked devices, include an array of security features and functions. This document will discuss the security features of Lexmark MFPs, describe the benefits, and provide instructions on implementation.

When connecting a device to your network, you must evaluate the security requirements necessary to ensure designed functionality. Things to consider include:

1. How can we protect the device from unauthorized access?
2. What are the vulnerabilities of installing an MFP device on the network?
3. What information will the device process and what are the security considerations related to that data?

These, and many other questions, are appropriate to ask before connecting any device to your network, including networked MFPs.

Lexmark MFPs operate independently on networks, which means that like networked computers and servers, they are capable of distributing information that may be sensitive in nature. Establishing security standards on the MFP is comparable to securing these types of networked devices. The requirements for managing network access, and the need for secure remote management, are largely the same for MFPs and workstations.

In other respects, however, the security considerations for MFPs are substantially different. MFPs do not run traditional operating systems and as a result, user authentication is applied differently. Furthermore, Lexmark MFPs do not have network file shares that need to be secured, therefore the devices do not need to support antivirus software.

This document will define the major topics of securing Lexmark MFPs and provide an overview of the security features and functionality that allow the devices to be deployed, managed and used in a secure manner on your network.

Applicability

This white paper applies to the following Lexmark products:

Lexmark X463de MFP	Lexmark X652de MFP	Lexmark X738de MFP	Lexmark X792dtme MFP
Lexmark X464de MFP	Lexmark X654de MFP	Lexmark X738dte MFP	Lexmark X792dtse MFP
Lexmark X466de MFP	Lexmark X656de MFP	Lexmark X792de MFP	Lexmark X860de 3/4 MFP
Lexmark X466dte MFP	Lexmark X658de MFP	Lexmark X792dte MFP	Lexmark X862dte 3/4 MFP
Lexmark X466dwe MFP	Lexmark X734de MFP	Lexmark X792dtfe MFP	Lexmark X864dhe 3/4 MFP
Lexmark X651de MFP	Lexmark X736de MFP	Lexmark X792dtpe MFP	Lexmark X925de 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 manage a fleet of networked MFPs, remote management is desired; however, the remote management must also be a secure process. The device should allow authorized personnel to configure it while rejecting users who are not authorized. Additionally, the process of managing the device must be secured so that the network traffic associated with its remote management cannot be sniffed, stolen or abused.

Lexmark MFPs include a host of features that make device remote management easier and more secure.

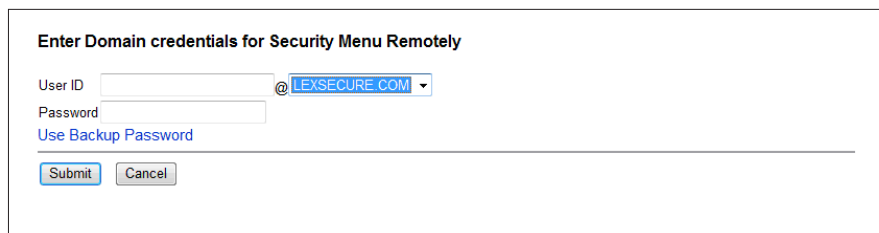
Function Access Controls, Authentication/Authorization, and Backup Passwords

Overview

The ability to change the device settings can be controlled through the use of function access controls, authentication/authorization mechanisms, and the backup password. This keeps unauthorized users from altering the device's settings, including security settings.

Lexmark MFPs support user authentication and authorization functionality. This allows device administrators to select individual users and/or appropriate groups to make changes to a device based on the MFP's function and access rights. With this functionality, individual users as well as users who are part of a group will be able to use their network user name and password credentials to access the device (see Figure 1). The device will determine whether the user has appropriate access, based on the rights configured by the network administrator. This level of control applies to network access via the device's Web server, as well as to configuration of the MFP through the operator panel.

Additionally, Lexmark MFPs can be set up by the device administrator to have a backup password. This password provides access to the device's security menu when the MFP has limited or no access to network directory servers. The password is designed to give the administrator access to the device so that temporary changes can be made to the MFP's function access controls.



Enter Domain credentials for Security Menu Remotely

User ID @ LEXSECURE.COM

Password

[Use Backup Password](#)

Figure 1: When an attempt is made to configure the MFP via the Web browser, the appropriate user ID and password must be provided.

Benefits

Through the use of function access controls and network authentication/authorization mechanisms, Lexmark MFPs can be configured to allow local access to settings and functions for one or more authorized users or groups while reserving remote configuration over the device's settings for authorized administrators.

Support for a backup password is a basic building block of security. It allows access to the MFP's security menu in times when the device's network connection is down or lost. This also allows the device's security menu to be protected while administrators configure the device during the initial setup process.

Details

The MFP supports a backup password that can be created during the initial setup of the device and can be used in the event of limited or loss of network communication. The backup password provides global control over all of the MFP's security menu settings. The backup password 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. While the backup password allows an administrator to protect the device during the initial configuration of the MFP's security settings and provides local access to the device if network connectivity is lost, it does not give access to the MFP's operating system or hard disk drive. The operating system and the device's file system are not exposed to external configuration by any means.

While the backup password is used during initial device configuration and/or during the loss of connectivity of the device, the primary means of device access, by users and/or administrators, should be done through the use of network user accounts (which are located on a corporate directory server) or through the use of local user accounts (which are located on the device). By requiring users and administrators to provide credentials for authentication, device administrators can configure the MFP to determine access based on user/group needs and/or rights¹. The ability to determine access is done through a combination of function access controls, security templates, and authentication/authorization mechanisms (see page 19) which are configured by the device administrator.

Device function access controls (see Figure 2), are settings that can be configured to allow local and remote access to the MFP's functions/menus. Each of the MFP's functions/menus can be configured to use one of the following settings: No Security (default setting), Disabled (if the function can be disabled), or Restricted (through the use of the authentication/authorization mechanism setup by a device administrator).

¹ The backup password is not associated with any accounts in the corporate directory; it is a password that is stored only on the MFP. This password should only be shared with those users who are authorized to modify the corresponding device's security settings.

Settings

Edit Access Controls

Choose a Security Template to protect each function

Functions which can be disabled have a 'Disabled' selection. To let anyone use the function, choose 'No Security'.

Security Menu at the Device	GSSAPI_Admin
Security Menu Remotely	GSSAPI_Admin
Service Engineer Menus at the Device	GSSAPI_All_Admins
Service Engineer Menus Remotely	GSSAPI_Admin
Configuration Menu	Gibbons
Operator Panel Lock	GSSAPI_All_Admins
Change Language from Home Screen	GSSAPI_Print_Tech
Paper Menu at the Device	GSSAPI_All_Users
Paper Menu Remotely	No Security
Reports Menu at the Device	GSSAPI_All_Users
Reports Menu Remotely	GSSAPI_All_Admins
Settings Menu at the Device	GSSAPI_Print_Tech
Settings Menu Remotely	GSSAPI_Print_Tech
Network/Ports Menu at the Device	GSSAPI_All_Admins
Network/Ports Menu Remotely	GSSAPI_All_Admins
Manage Shortcuts at the Device	GSSAPI_All_Users
Manage Shortcuts Remotely	GSSAPI_All_Users
Flash Drive Print	GSSAPI_All_Users
Flash Drive Scan	GSSAPI_All_Users
Flash Drive Firmware Updates	GSSAPI_Admin
Web Import/Export Settings	GSSAPI_All_Admins
Copy Function	No Security
Color Dropout	No Security
E-mail Function	GSSAPI_Admin
Fax Function	GSSAPI_All_Users
Release Held Faxes	GSSAPI_All_Users
FTP Function	GSSAPI_All_Users
Held Jobs Access	GSSAPI_All_Admins
Use Profiles	GSSAPI_All_Users
Create Bookmarks at the Device	GSSAPI_All_Users
eSF Configuration	GSSAPI_All_Admins
Remote Management	GSSAPI_All_Admins
Firmware Updates	No Security
Solution 1	GSSAPI_All_Users
Solution 2	GSSAPI_All_Users
Solution 3	GSSAPI_All_Users
Solution 4	GSSAPI_All_Users
Solution 5	GSSAPI_All_Users
Solution 6	GSSAPI_All_Users
Solution 7	GSSAPI_All_Users
Solution 8	GSSAPI_All_Users
Solution 9	No Security
Solution 10	No Security
Option Card Configuration at the Device	GSSAPI_Admin
Option Card Configuration Remotely	GSSAPI_Admin
Address Book	GSSAPI_All_Users
Create Profiles	GSSAPI_All_Users
Create Bookmarks Remotely	GSSAPI_All_Users
PJL Device Setting Changes	Disabled
NPA Network Adapter Setting Changes	No Security

Submit Reset Form

Figure 2:
This example shows the various function access controls mentioned in this document.

HTTPS

Overview

The most common means to remotely configure network devices, including Lexmark MFPs, is through the device's Web interface. You can figure device settings by pointing a browser to the MFP's IP address or DNS name and providing the proper credentials (as described above in Function Access Controls, Authentication/Authorization, and Backup Passwords).

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

Benefits

The benefits of using HTTPS for Web sessions include:

1. 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.
2. Encryption of all data exchanged through the browser, this includes passwords and any other settings that are set or viewed.
3. Support by most commonly used Web browsers; HTTPS and SSL are extremely prolific standards.
4. Integration into pre-existing certificate authority (CA) or public key infrastructure (PKI) environments; the MFP's certificate that allows the SSL session to be established can be signed by a certificate authority.

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 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 will not receive 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 session.

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

Simple Network Management Protocol (SNMP) provides another means to remotely configure MFPs. Because SNMP can be used to both view and modify MFP settings, the basic security questions of how to control its use and how to protect the associated network traffic when it is used are relevant.

Lexmark MFPs support the latest version of SNMP (currently SNMPv3). They also support SNMPv1 and v2 for backward compatibility. The standard protocol includes support for authentication and data encryption.

Benefits

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

1. Authentication allows authorized systems to see and manage the MFP via SNMPv3, while shutting out unauthorized systems.
2. Encryption of the SNMPv3 packets protects the information from being sniffed while on 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 valid digital signatures, such as 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. See Figure 3 for more detailed setup information.

SNMP Version 1,2c	
Enabled	<input checked="" type="checkbox"/>
SNMP Set Enabled	<input checked="" type="checkbox"/>
SNMP Community	<input type="text" value="public"/>
SNMP Version 3	
Enabled	<input checked="" type="checkbox"/>
SNMPv3 Read/Write User	<input type="text" value="AcmeAdmin"/>
SNMPv3 Read/Write Password	<input type="password" value="*****"/>
SNMPv3 Read Only User	<input type="text" value="AcmeReader"/>
SNMPv3 Read Only Password	<input type="password" value="*****"/>
SNMPv3 Minimum Authentication Level	<input type="text" value="Authentication, Privacy"/>
SNMPv3 Authentication Hash	<input type="text" value="MD5"/>
SNMPv3 Privacy Algorithm	<input type="text" value="DES"/>

Figure 3: SNMPv1 and SNMPv2 can be enabled or disabled independently of SNMPv3. SNMPv3 supports both authentication and privacy features.

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

IP Security (IPSec)

Overview

IP Security (IPSec) is supported on Lexmark MFPs. This is an extremely important mechanism, because 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, such as Windows and Linux. 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:

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

3. 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 provides a redundant level of security. Alternately, IPSec can be configured to be the only security mechanism, simplifying the security setup.
4. Protection of all traffic between Lexmark's device management application, MarkVision Professional, 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 MFPs 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 with up to five other systems or subnets. This allows the MFP to exchange data securely with a large number of systems, and allows the process to be integrated with a PKI or CA infrastructure. The use of certificates 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 is 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 pre-shared key mode and certificate mode, simultaneously.

802.1x Support

Overview

In almost all network environments, users are required to log on to the network before they can send or receive e-mail, browse the Web, or initiate other tasks. Increasingly, it is important to require devices such as laptops or MFPs to authenticate before allowing them access to the network. The protocol for performing this authentication is 802.1x. Lexmark MFPs support the 802.1x protocol for device authentication.

Benefits

802.1x provides the following benefits:

1. It allows the MFP to authenticate itself on the network, increasing security.
2. With support for a wide array of authentication methods, the 802.1x authentication mechanism is compatible with almost any 802.1x authentication environment.
3. 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 edge devices and 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 network device is the process of securing the device's network interfaces. Not only can device hardening eliminate unneeded or unused to prevent their abuse, but it can also lock down any interfaces that remain and can secure the data hosted by the device.

Lexmark MFPs include a variety of mechanisms to facilitate the device hardening process.

Port Filtering

Overview

Port filtering is implemented on Lexmark MFPs 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 regarding which protocols are and are not allowed on the network.

Benefits

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

1. Increased security. Provides granular and authoritative control over protocols the device processes or ignores.
2. Cleaner port scans. By shutting down unneeded ports, the port scans will not report “phantom” vulnerabilities that need to be tracked down and understood.
3. Enhanced redundancy. Many protocols (such as HTTP, FTP and others) can be disabled at two different locations on the MFP’s Web server: the TCP/IP settings section (under the Network/Ports menu) and the TCP/IP Port Access settings section (under the Security menu).
4. Reduced network traffic.

Details

The MFP allows each of 28 TCP and UDP ports to be individually opened or closed:

TCP 21 (FTP)	TCP 6110/UDP 6110/TCP 6100
UDP 69 (TFTP)	TCP 8000 (HTTP)
TCP 79 (FINGER)	TCP 9000 (Telnet)
TCP 80 (HTTP)	TCP 9100 (Raw Print)
TCP 443 (HTTPS)	TCP 9200 (IR Alerts)
UDP 137 (WINS)	UDP 9200 (Discovery)
UDP 161 (SNMP)	UDP 9300/9301/9302 (NPAP)
UDP 162 (SNMP Traps)	TCP 9400 (Enhanced Print Port)
TCP 515 (LPR/LPD)	TCP 9500/TCP 9501 (NPAP)
TCP 631 (IPP)	TCP 9600 (IPDS)
UDP 1584 (HBN1)	UDP 9700 (Plug-n-Print)
TCP 5000 (XML)	TCP 10000 (Telnet)
TCP 5001 (IPDS)	ThinPrint
UDP 5353 (MDNS)	Web Services

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

Hard Disk Encryption

Overview

A common concern for networked devices is that data will be exposed to remote access. 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 disk 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 image scans or print jobs that the MFP receives.

Lexmark MFPs can encrypt all data on the hard disks to protect the device from external access at all times. When this feature is enabled, all data written to the hard disk is encrypted. This protects not only residual data left over after jobs, but it 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 disk.

Benefits

The benefits of hard disk encryption include:

1. Increased security of active and residual data.
2. The hardware-assisted encryption is applied in real time, so there is no delay for cleanup or post-processing after jobs have completed.
3. A dynamically generated encryption key stored on the MFP (not the hard disk) makes the data on an encrypted disk drive useless on any other MFP². Removing the hard disk from the MFP will not yield access to the data it contains.

Details

By default the data on the MFP's hard disk is not encrypted. This does not mean the contents of the drive are exposed. Rather, encryption is unnecessary because there is no path by which residual job data can be retrieved or accessed remotely³.

When hard disk encryption is activated, the encryption key to be used (256 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 disk itself, so if the hard disk was stolen from the MFP, the contents of the hard disk would remain indecipherable.

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

² Note that this does not render the hard disk drive useless. When an encrypted hard disk is moved from one MFP to another, it must be reformatted when it is placed into the new MFP. The hard disk is portable, but the data on it is not.

³ There are many factors that lead to this—more than are pertinent for this white paper. Briefly, however, there is no means by which to have the MFP reprint or retrieve residual data as the MFP does not support a network file system or file sharing. Further, there is no protocol supported by the MFP that allows someone to arbitrarily read or write data to or from the hard disk. Even without encryption of the disk's data, the contents are well protected.

Hard Disk Wiping

Overview

When a data file is “deleted” from a hard disk, the data that is associated with that file is not actually deleted. This data remains on the hard disk and could theoretically be recovered, albeit with substantial effort.

Lexmark MFPs support an additional mechanism for protecting residual data: hard disk wiping. Hard disk wiping actively overwrites the entire hard disk drive with multiple passes of data, removing all residue of prior information. Lexmark MFPs have support for the following types of hard disk wiping: automatic, scheduled, manual, and out-of-service.

Benefits

The benefits of hard disk wiping include:

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

Details

The MFP’s hard disk is used exclusively for buffering data, such as scanned data, incoming print jobs, and any other image data related to job processing. Depending on the type of wiping process, the hard disk can be wiped of all its contents, or it can be wiped only of residual data left over from buffered jobs (print, copy, fax, and/or scan).

The hard disk wiping process can be set up to automatically wipe data after it has been used; scheduled to conduct a wipe during a certain time, day, week, or month; or activated manually through the device’s operator panel. Additionally, the MFP has an out-of-service wipe that can be activated through the device’s configuration menu. The out-of-serve wipe is designed to completely sanitize all data, including fonts, forms, embedded solutions, and buffered jobs.

Lexmark’s wiping process adheres to National Institute of Standards and Technology (NIST) and U.S. Department of Defense (DoD 5220.22-M) guidelines for overwriting confidential data on a device’s hard disk drive multiple times with complementary data followed by random data.

TCP Connection Filtering

Overview

Lexmark MFPs 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:

1. Approved systems, such as print servers and administrative workstations, are allowed to make connections to the MFP, allowing normal and approved functions, such as printing and routine monitoring and maintenance, to occur normally.
2. 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 print subsystem. All of these connections will be allowed only to/from the specified systems.
3. End-user systems can be omitted from the list, which prohibits them from connecting to the MFP via a Web browser or FTP connection.
4. Any system that is not listed is refused access, securing the MFP against unauthorized external connections.

Details

The restricted server list (shown in Figure 4) 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.

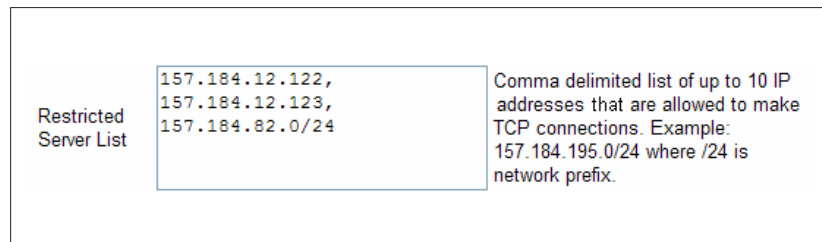


Figure 4: The restricted server list allows individual addresses and subnets to be specified. TCP connections from all other addresses will be refused by the MFP.

The restricted server list does not affect UDP traffic, therefore 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 an intruder 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 is no exposure of this sort on Lexmark's MFPs. The fax modem allows for the exchange of facsimile images only. There is no path by which the fax modem connection can interact with or control the MFP's network interface, and there is no facility for configuring the MFP's settings via the fax modem connection. The fax modem connection simply allows one to send and receive fax images, nothing more.

Benefits

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

1. Incoming fax images can be printed as hardcopy documents or routed to a predefined e-mail, 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.
2. Incoming faxes can be redirected to an alternate fax machine. This could be useful when an office is temporarily closed, by allowing incoming faxes to be forwarded to an alternate device that is 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, rather, the information exchanged over the MFP's modem is restricted to image data only.

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

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

Digitally Signed Firmware Updates

Overview

Lexmark MFPs support a firmware download mechanism. This enables the firmware that controls the device's behavior to be updated. This is a common and appropriate feature, useful for feature upgrades or issue resolution. However, it is important that these firmware updates are carefully controlled to avoid any exposure to unauthorized code being placed on the device.

Lexmark MFPs perform multiple checks on downloaded firmware before adopting the firmware or executing any code contained in the package. This prohibits someone 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:

1. The MFP's capabilities can be maintained and extended through the application of appropriate and authorized firmware updates.
2. 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 MFPs 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, through a key that is known only to Lexmark and is embedded securely in all MFPs. However, 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 since the signatures were applied, the firmware is discarded.

Firmware updates can be transmitted over the network, which allows the devices to be updated en masse. This process can be automated and scheduled, and the process does not require someone 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 afterward.

Lexmark MFPs support custom Java applications through an embedded application platform. These Java applications must also be digitally signed by Lexmark before being adopted. This prohibits users from placing unauthorized applications on Lexmark MFPs.

Secure Device Operation

Lexmark MFPs include standard features to secure the use of the device, ensuring only appropriate personnel 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 left on the MFP for anyone to pick up. With Confidential Print, the MFP securely holds submitted jobs until the intended recipient is present at the device and enters the proper PIN code on the MFP's operator panel.

Benefits

The features and benefits of Confidential Print include:

1. An intuitive and effective means to deliver print jobs only when the recipient is at the MFP.
2. Security is provided with four-digit PINs from 0000-9999, which provides up to 10,000 possible values.
3. 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.
4. 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 disk encryption is enabled (see page 12), the stored jobs will be encrypted for additional security.
5. 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 MFPs.

When the MFP receives a Confidential Print job, the datastream is stored on the MFP's RAM memory or on the MFP's hard disk. Jobs stored in the MFP's RAM memory will be deleted if the MFP is powered off. Jobs stored in RAM memory can also 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, greatly increasing the number of jobs that can be held by the MFP.

Jobs buffered to the MFP's hard disk can leverage the security of hard disk encryption. As discussed on page 12, buffered data on an encrypted hard disk cannot be processed if that hard disk is moved to another MFP. Furthermore, the hard disk itself cannot be used by the other MFP without being reformatted.

For additional security, setting a maximum number of retries on PINs (shown in Figure 5) 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.

Confidential Print Setup

Max Invalid PIN Range: 2 - 10, Off = 0.

Job Expiration ▼

Figure 5: 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.

Additionally, 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 and Authorization

Overview

When a user approaches the MFP and selects a function such as Scan to E-mail, the MFP can require the user to authenticate before proceeding. This limits access to the device to valid users and allows the MFP to identify the user performing the function.

As mentioned earlier in this document, Lexmark MFPs support not only user authentication, but authorization as well. This allows device administrators to grant individual users and/or appropriate groups the right to access a particular device function or functions, while restricting other users and/or groups from using the same function(s). With this functionality, individual users or group members are able to use their network username and password to access the device. The MFP will determine whether the user has access to the appropriate function(s) based on the access rights configured by the device administrator. This level of control applies to network access via the device's Web server, as well as to configuration and use of the MFP through the touch screen interface.

An important aspect of user authentication and authorization is allowing users to enter their "normal" user ID and password. A user should not, and does not, need to remember a special set of information to use the MFP. Instead, the MFP makes use of the corporate directory to validate a user's credentials against the standard, centralized database.

Benefits

The benefits of user authentication and authorization include:

1. Securing the MFP by limiting who can use its scan to network capabilities.
2. Anonymous e-mail is avoided by inserting the identity of the authenticated user into e-mail generated by the scan to e-mail function. With additional configuration, scan to e-mail can also limit e-mails to a predetermined destination (for example, "@company.com") so that e-mail cannot be sent to arbitrary destinations.
3. When users authenticate, they use their normal login and password, just as if they were logging onto their workstation or laptop. This keeps the process simple and intuitive.
4. Faxes sent via networked fax servers can automatically send an e-mail confirmation of the fax to the sender's e-mail, since the MFP "knows" who is sending the fax.

Benefits

As mentioned in the Function Access Controls, Authentication/Authorization, and Backup Passwords portion of this document (see page 4), the MFP can be set up to restrict access to over 50 functions, including the following walk up functions:

- Copy
- Scan to E-mail
- Scan to Fax
- Scan to FTP
- Print held jobs (such as Confidential Print jobs)
- The ability to print jobs from a portable USB memory device (thumb drive")
- The ability to scan jobs to a portable USB memory device
- Launching embedded applications

Note that access to these functions can be set by a particular authentication building block and security template. Additionally, a function access control can be set to either of the following levels:

- No Security –Wide open access, so that anyone can use the device without any authentication. This is appropriate when no control or tracking is necessary.
- Disabled – Each function can be disabled entirely in an environment where the given function is not needed or not appropriate. Disabled functions are not displayed on the MFP touch screen.

The process of authenticating users is flexible. The MFP can use a variety of device internal authentication mechanisms and network directory authentication mechanisms and protocols to validate user credentials. Through the use of authentication building blocks, Lexmark MFPs can be set up to use Device Internal Accounts, Device Passwords, Device PINs, LDAP (with or without SSL/TLS), Kerberos, LDAP+GSSAPI, and/or NTLM for authenticating users.

Support for a wide array of authentication protocols means that the MFP's user authentication function is compatible with an array of network environments, including Microsoft's Active Directory, Novell's eDirectory, and other directory environments that supports LDAP.

Secure user authentication protocols, such as LDAP with SSL/TLS configured, Kerberos, LDAP+GSSAPI, and NTLM, protect users' credentials during the authentication process.

Address Book Lookup via LDAP over SSL

Overview

When performing a Scan to E-mail or Scan to Fax operation, users can look up the recipient's e-mail address or fax number, rather than manually typing it. This important convenience feature is made possible through LDAP. LDAP allows the MFP to query the corporate directory for information.

The use of the Secure Sockets Layer (SSL) protocol 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:

1. The information queried by the MFP is secured (encrypted) on the network.
2. 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 CA 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 its 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 queries for e-mail and fax information, as well as LDAP-based user authentication.

Operator Panel Lock

Overview

The Operator Panel Lock feature allows an MFP to be put in a locked state so that the operator panel cannot allow any user operations or configuration. 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. If the MFP has a hard disk, incoming print and fax jobs are stored on the hard disk instead of being printed. The MFP can be unlocked by entering an authorized user's credentials, at which time the held jobs will be printed and the MFP will resume its normal operation.

Benefits

The features and benefits of MFP lockout include:

1. A simple method of securing the MFP during off hours by disallowing scanning and printing operations.
2. Jobs printed to a locked MFP cannot be stolen from the output bin.

Details

The operator panel lock is configured by creating an authentication building block and applying it against the Operator Panel Lock function access control via the MFP's embedded Web page. Depending on the type of authentication building block and the security template that is applied to this function access control, a user could enter a device PIN, a device password, or network credentials to lock or unlock the MFP at its operator panel. This feature requires that a hard disk be installed.

When the MFP is locked, the operator panel does not allow any interaction other than specifying the appropriate credentials 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 they are available through the typical Confidential Print jobs interface on the MFP's operator panel.

USB Device Restrictions

Overview

Lexmark MFPs support portable USB memory devices or "thumb drives" for printing and scanning. Users 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 portable USB memory devices include:

1. Disallowing users to perform scan-to-USB operations in environments where sensitive documents must be carefully controlled.
2. Disallowing users to perform print-from-USB operations in environments where printing is tracked or allowed only on a fee-basis.
3. Limits the ability to perform scan-to or print-from USB devices only to authenticated users.

Details

The MFP allows portable USB memory devices or “thumb drives” to be used for scan-to-USB or print-from-USB tasks. The MFP’s configuration cannot be set or recorded via USB devices.

The ability to scan-to or print-from USB devices can be controlled separately by a particular authentication building block and security template or set independently to any of the following states:

- No Security – The functions are active, and no authentication is required. This is appropriate for environments where no control or tracking is necessary.
- Disabled – The MFP won’t allow print from and/or scan to USB devices.

Summary

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

Lexmark MFPs are equipped with an array of security features that allow you to secure networked MFP devices and their use. All three primary layers of security are addressed:

1. Lexmark MFPs can be managed securely through the use of authentication/authorization mechanisms, HTTPS, SNMPv3, and IPSec.
2. Lexmark MFPs can be hardened with port filtering, TCP connection filtering, hard disk encryption, and hard disk wiping.
3. Lexmark MFPs can be operated securely with secure user authentication/authorization, address book lookups via LDAP over SSL, a Confidential Print feature, and operator panel lockout.

About Lexmark International

Lexmark International, Inc. (NYSE: L XK) makes it easier for businesses and consumers to move information between the digital and paper worlds. Since its inception in 1991, Lexmark has become a leading developer, manufacturer and supplier of printing and imaging solutions for customers in more than 170 countries.

Lexmark's enterprise sales force is organized into industry-specific vertical teams that identify the unique challenges of each major industry in terms of output and workflow processes. Our solutions and customer-focused approach is what makes us different in the market, but our award-winning products are at the heart of our business. Lexmark is the only office solution manufacturer that internally develops and owns all of our core technologies in the market. We pride ourselves on understanding our customer's specific needs and developing innovative solutions to meet those needs.

For more information about Lexmark's document solutions, please visit our website at www.lexmark.com.

Copyright © 2010 Lexmark International, Inc. All rights reserved.

Lexmark reserves the right to change specifications or other product information without notice. References in this publication to Lexmark products or services do not imply that Lexmark intends to make them available in all countries in which Lexmark operates. LEXMARK PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. This publication may contain third party information or links to third party sites that are not under the control of or maintained by Lexmark. Access to any such third party information or site is at the user's own risk and Lexmark is not responsible for the accuracy or reliability of any information, data, opinions, advice or statements made by these third parties. Lexmark provides this information and links merely as a convenience and the inclusion of such information and/or links does not imply an endorsement. All performance information was determined in a controlled environment. Actual results may vary. Performance information is provided "AS IS" and no warranties or guarantees are expressed or implied by Lexmark. Buyers should consult other sources of information, including benchmark data, to evaluate the performance of a solution they are considering buying.