

Lexmark Security



LEXMARKTM

Lexmark Security

Security Function Overview – The following security functions are available on Lexmark’s products.

Confidential Print

Print jobs are held in RAM or on hard disk until the intended recipient enters the appropriate PIN, which causes the job to be printed. Held jobs can be set to expire after an elapsed time (configurable from one hour to one week), and a limit on the number of times a PIN can be entered incorrectly can be set before the corresponding jobs are purged.

Operator Panel Lock

On printers, the operator panel can be locked in part or entirely, requiring a PIN to access restricted menus.

On MFPs, access to the configuration menus via the operator panel can be restricted. The access can be disallowed entirely, or restricted to administrators through the use of the Administrative Password Protection function.

Administrative Password Protection

Printers and MFPs support the creation of an administrative password.

For printers, all web-based configuration of the device requires the password to be provided—without the password, one cannot view or change the device’s settings.

For MFPs, configuration of the device by the web interface and the MFP’s touch screen are both covered by the administrative password.

TCP Connection Filtering

Printers and MFPs can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses. This disallows all TCP connections from other addresses, which protects the device against unauthorized printing and configuration.

Network Port Filtering

The network ports on which printers and MFPs listen for or transmit network traffic can be configured, allowing a huge degree of control over the device’s network activity.

By filtering out traffic on specific network ports, protocols such as telnet, FTP, SNMP, HTTP, and many others can be explicitly disallowed.

Hard Disk Encryption

Hard disks in printers and MFPs can be configured to use encryption. A 128-bit AES key is internally generated by the printer or MFP and used to encrypt all data on the drive.

The key is stored non-contiguously on the device, making the contents of the drive accessible only on the drive’s original printer or MFP. The data on a stolen drive would not be accessible, even if it were installed in an identical model of printer or MFP.

Hard Disk Wiping

MFPs support hard disk sanitization, where the contents of the internal hard disk can be erased by overwriting the entire disk, eliminating all residual data.

Printer Lockout

Printers can be locked, so that the printer’s front panel is disabled and all incoming print jobs are stored securely on the printer’s hard drive until the printer is unlocked by entering the appropriate PIN. This feature is available on printers that are equipped with a hard drive.

MFP Lockout

MFPs can be locked, so that the MFP’s touch screen is disabled and all incoming print and fax jobs are stored securely on the MFP’s hard drive until the MFP is unlocked by entering the appropriate PIN. This feature is available on MFPs that are equipped with a hard drive.

Incoming Fax Holding

MFPs can be configured to hold, rather than print, incoming faxes during scheduled times. Incoming faxes are held securely on the MFP’s hard drive until a predefined password is entered.

SNMPv3

SNMP is a standard network management protocol, and version 3 (SNMPv3) includes extensive security capabilities. Lexmark’s printers and MFPs support SNMPv3, including the authentication and data encryption components, allowing for secure remote management of the devices.

Note that SNMPv1/v2 are also supported, and can be independently configured and/or disabled.

Lexmark Security

HTTPS

HTTPS provides a means to securely manage networked printers and MFPs. It allows web traffic to be encrypted, so that remote management via the printer and MFPs web pages can be performed securely.

IPSec

IPSec allows all network traffic to and from printers and MFPs to be secured with encryption and authentication. This allows data to be sent to printers and MFPs securely, and allows scanned jobs to be transferred securely from MFPs.

IPv6

IPv6 is supported on printers and MFPs to allow connectivity to IPv6 networks.

802.1x

802.1x port authentication allows printers and MFPs to join networks that require devices to authenticate prior to accessing the network. 802.1x port authentication can be used with the WPA (Wi-Fi Protected Access) feature of an optional wireless print server to provide WPA-Enterprise security support.

Certificate Management

Printers and MFPs use certificates for HTTPS, SSL, IPSec, and 802.1x authentication. The certificate management feature of printers and MFPs allow the devices to integrate with a PKI environment by allowing the device's certificates to be signed, and by allowing the printers and MFPs to trust certificate authorities in the customer's PKI environment.

Digitally Signed Firmware Updates

Printers and MFPs automatically inspect downloaded firmware upgrades for the appropriate Lexmark digital signatures. Firmware that's not correctly packaged and signed by Lexmark is rejected. This ensures that non-approved firmware is never run on the devices, which avoids exposing the printers and MFPs to malicious software such as viruses and worms.

Compatible with Physical Locks

Printers and MFPs support Kensington-style locks, which allow the devices to be physically secured. Locking a printer or MFP also locks down the metal cage that houses hard drives and optional components, preventing those components from being tampered with or stolen.

Secure User Authentication

MFP functions can be restricted so that users must authenticate prior to performing copy, scan to email, scan to fax, scan to network, workflow scripts, or embedded applications. MFPs can be configured to authenticate users against the customer's corporate directory via LDAP, LDAP over SSL, Kerberos, or NTLM. These authentication methods are secure, and compatible with Active Directory and other directory server platforms.

LDAP Address Book Lookup

When sending emails or faxes, users can look up the recipient's email addresses and fax numbers. The MFP uses LDAP to perform the lookups, by directing LDAP queries to the customer's corporate directory server.

Secure LDAP over SSL

All LDAP traffic to and from MFPs can be secured with SSL. Exchanging LDAP over an SSL connection means the information exchanged via LDAP, including the user's credentials, names, email addresses, and fax numbers, is encrypted to preserve the confidentiality and privacy of the data.

Auto-Insertion of Sender's Email Address

When a user authenticates on an MFP in order to send a scan to email job, the email address of the sender is automatically looked up by the MFP and inserted into the "From:" field of the scan to email job. This means that the recipient can clearly see that the email was generated by the individual that sent the job. The resulting email is not anonymous, or attributed to the MFP itself.

Encrypted Scan

The use of IPSec allows scanned data to be transmitted over the network in an encrypted format. This can protect the contents of jobs that are scanned to any destination, including LDD, email, and network storage. All scanned data and all associated data can be encrypted through the IPSec protocol.

Lexmark Security

Security Function Availability

Printers

	Confidential Print	Operator Panel Lock	Administrative Password Protection	TCP Connection Filtering	Network Port Filtering	Hard Disk Encryption	Printer Lockout	SNMPv3	HTTPS	IPSec	IPv6	802.1x	Certificate Management	Digitally Signed Firmware Updates	Compatible with Physical Locks
E120n			•	•		n/a							n/a		
E240n			•	•		n/a							n/a		
E340			•	•		n/a							n/a		
E342			•	•		n/a							n/a		
T430			•	•		n/a							n/a		
T640	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
T642	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
T644	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
W840	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
C522n	•	•	•	•	•	n/a									
C524n	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
C920	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

MFPs

	Confidential Print	Operator Panel Lock	Administrative Password Protection	TCP Connection Filtering	Network Port Filtering	Hard Disk Encryption	Hard Disk Wiping	MFP Lockout	Incoming Fax Holding	SNMPv3	HTTPS	IPSec	IPv6	802.1x	Digitally Signed Firmware Updates	Compatible with Physical Locks	Certificate Management	Secure User Authentication	LDAP Address Book Lookup	Secure LDAP over SSL	Auto-Insertion of Sender's Email Address	Encrypted Scan
X340n, X342n	•												•									
X422	•	•	•	•	•	n/a	n/a								•							
X642e	•	•	•	•	•	n/a	n/a			•	•	•	•	•	•	•	•	•	•	•	•	•
X644e	•	•	•	•	•	n/a	n/a			•	•	•	•	•	•	•	•	•	•	•	•	•
X646e	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
X646dte	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
X646ef	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
X850e	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
X852e	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
X854e	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•