Lexmark Security Reference Guide

When it comes to security, your organization needs to ensure that it can securely manage network devices, defend them from hackers and physically protect the stored data. That's why at Lexmark, we've designed our solutions-capable printers and MFPs to answer these needs.

Full-spectrum security

Security is built into every Lexmark product, with standard security features appropriate to each product's intended use and available options to fulfill special requirements. Our comprehensive approach to Lexmark product security covers a full spectrum of security capabilities.

- **Secure access** features restrict who can use your devices and what they can do.
- **Network security** features protect devices from unauthorized access over network interfaces.
- **Document security** features keep your documents—whether physical or virtual—out of the wrong hands or views.
- **Secure remote management** provides a wide range of tools and device capabilities to effectively manage a fleet of networked laser printers and multifunction products.
- **Security solutions** enhance the security of Lexmark devices and your environment by meeting specific objectives like print release*, automatic security certificate and Secure Content Monitor.
- **Hard disk security** protects Lexmark printers and multifunction products that contain internal hard disks with a virtual shield to keep your organization's secrets.

*Optional

Secure access features

Who are you? Most digital security breaches depend on a user pretending to be someone they aren't. Lexmark devices are designed to provide unhindered access to the right users, while keeping out the pretenders.

Authentication and authorization flexibility: Lexmark devices can be configured to validate user credentials and restrict device functions using Active Directory and other directory server platforms, including internal accounts, NTLM, Kerberos 5, LDAP, LDAP+GSSAPI, password, and PIN.

User and group security: Grant individual users and sets of users the right to access particular device functions, while restricting other users or groups.

Access controls: Control local and remote access to specific menus, functions and workflows on each device. Entirely disable functions like copy, print, fax, scan to email, FTP, held jobs and address book. Over 50 access controls are available, providing greater flexibility for your unique environment.

Security templates: Device administrators can easily restrict device access by combining group privileges, access controls, and authentication methods into security templates that appear in the Access Control drop-down menu. The breadth that a security template can cover is large, providing control over some of the most important security settings on the Lexmark device.

Protected USB ports: Lexmark laser printers and MFPs include support for USB devices which may cause concern in environments where security is critical. Designed with security in mind, USB host ports have various mechanisms in place to keep them from being used in a malicious manner.

Auto-insertion of sender's email address: When a user authenticates in order to scan a document to email, the email address of the sender is automatically looked up and inserted into the "From" field. This lets the recipient clearly see that the email was generated by that individual, not anonymously or from the MFP.

Login restrictions: You can prevent unauthorized use of a device by restricting the number of consecutive failed logins—and track such events through integrated auditing. When this limit is exceeded, the device is locked for a predetermined amount of time specified by the administrator.

Operator Panel Lock: 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. The device can be unlocked by entering an authorized user's credentials, allowing the device to resume its normal operation.

Incoming fax holding: Lexmark devices can be configured to hold rather than print incoming faxes during scheduled times. Incoming faxes are held securely on the hard disk until the proper credentials have been entered on the Lexmark device. Examples of credentials include a PIN, password, and user network ID and password.

Network security

Modern IT is built around the network, but the same connectivity that makes networked devices accessible to authorized users could put your network integrity and valuable information at risk without the technologies and safeguards built into devices from Lexmark.

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.

Port filtering: The network ports through which printers and MFPs listen for or transmit network traffic are configurable, 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.

802.1x: With 802.1x port authentication, printers and MFPs can join wired and wireless networks by requiring the devices to authenticate prior to accessing the network. This authentication can be used with the Wi-Fi Protected Access feature of an optional wireless print server to provide WPA Enterprise security support.

IPsec: The IPsec protocol option, when enabled, secures network traffic to and from Lexmark devices with encryption and authentication. This protects print data and the contents of jobs that are scanned to any destination, including servers running Lexmark Document Distributor, email, and network storage.

Secure NTP: Lexmark devices support the use of Secure Network Time Protocol (SNTP) to sync clocks of various devices on the network. To support the main requirement for an SNTP implementation, Lexmark devices support an Authenticator and Authorization field within our SNTP configuration.

Fax/network separation: Lexmark offers a variety of MFP devices that provide both network connectivity and fax modem capability. And to prevent any direct interaction between the modem and network adapter, Lexmark device hardware and firmware keep these mechanisms separate.

Secure LDAP: All LDAP traffic to and from Lexmark devices can be secured with TLS/SSL. LDAP information such as credentials, names, email addresses and fax numbers exchanged over a TLS/SSL connection ensures the information is encrypted to preserve the confidentiality and privacy of data.

Document security

Traditionally, people clicked "print" from their desks and network printers cranked out and stacked up pages, keeping secrets about as well as the lunchtime crowd in a small-town cafe. Knowing you need to print many documents but still secure the information they contain, Lexmark offers a variety of features and optional products that make sure only authorized eyes see private output—while saving paper and consumables and giving mobile users new printing choices. It's the Lexmark way to fortify document security.

Confidential Print: A standard part of the Lexmark Universal Print Driver, Confidential Print holds your job on a specific Lexmark printer or MFP until you release it with a PIN, preventing prying eyes from viewing documents in the output bin. Held jobs can be set to expire after an elapsed time (configurable from one hour to one week). In addition, a limit can be set on the number of times a PIN can be entered incorrectly before the corresponding jobs are purged. Like all forms of print release, you only pay for actual pages printed—not the ones someone printed but never picked up.

Secure Held Print Jobs application: Prevent the accidental exposure of your sensitive or confidential business information by holding jobs at a specific device until an authorized user walks up and releases the job for printing. That's the basic premise of the Secure Held Print Jobs eSF app* for smart devices, which lets users send and store jobs on the printer or MFP and release them at their convenience using a four-digit PIN or ID card.

Secure print release: Lexmark Print Management* lets users send jobs from anywhere and pick them up at any print release-configured device on your network. You'll improve printing flexibility, avoid having documents piling up on printers, protect the confidentiality of documents that would otherwise be out in the open, and save on printing costs. And the whole release process is secured by credentials entered at the device, in the form of network user identification or an ID badge.

Options like that help Lexmark bring document security to every print job and every workflow.

*Optional

Secure remote management

To practically manage a fleet of networked print and imaging devices, secure remote management is a must. The device must allow authorized people to configure it, while rejecting those that are unauthorized. The process of managing the device must also be secured so that the network traffic associated with the remote management can't be sniffed, stolen or abused.

Lexmark devices include a variety of features to make remote device management easier and more secure. These features can be configured through the device's embedded Web page.

Device and settings access: What makes Lexmark smart printers and multifunction products (MFPs) smart is their ability to run and configure apps that automate manual tasks, enhance security and guide users through your business processes with ease. But like any programmable devices with comprehensive configuration options, they should be as carefully protected as any PC or server on your network. Lexmark devices include a variety of function access controls, authentication and authorization mechanisms and an optional backup password to keep unauthorized users from altering the device's settings, including security settings.

Audit logging: Track security-related events to mitigate exposure, proactively track and identify potential risks, and integrate with your intrusion detection system for proactive real-time tracking.

Encrypted and digitally signed firmware: Lexmark printers and MFPs automatically inspect downloaded firmware updates for the appropriate Lexmark digital signatures. Firmware that's not correctly packaged and signed by Lexmark is rejected.

Secure boot technology validates that the firmware installed on the printer is genuine Lexmark firmware. Should non-genuine firmware be detected, users receive notification.

Continuous verification ensures the firmware has not been tampered with during operation.

Certificate Management: Printers and MFPs use certificates for HTTPS, SSL, IPsec, and 802.1x authentications. The Certificate Management feature allows the devices to integrate with a PKI environment by allowing the certificates to be signed, and also allows the devices to trust certificate authorities in the PKI environment.

HTTPS: Lexmark printers and MFPs use the HTTPS communication protocol. It allows Web traffic to be encrypted so that you can securely perform remote management via the device Web page.

SNMPv3: Version 3 of the standard network management protocol SNMP includes extensive security capabilities. Lexmark printers and MFPs support SNMPv3—including the authentication and data encryption components—to allow secure remote management of the devices. SNMPv1 and SNMPv2 are also supported and can be independently configured or disabled.

Secure password reset: In the event that an administrative password is lost or forgotten, or the device has lost network connectivity, the secure password reset feature resets the access control setting on the device's security menu to allow access.

Security solutions

Your Lexmark laser printer or smart MFP can run security-related apps to fill special needs like print release*, automatic security certificate enrollment and smart card authentication. Another solution can centrally track and audit every document that's printed, copied, scanned or faxed on your network.

Secure print release: Lexmark Print Management* lets users send jobs from anywhere and pick them up at any print release-configured device on your network. You'll improve printing flexibility, avoid having documents piling up on printers, protect the confidentiality of documents that would otherwise be out in the open, and save on printing costs. And the whole release process is secured by credentials entered at the device, in the form of network user identification or an ID badge.

Automatic Certificate Enrollment (ACE): Creating a CA-signed device certificate to permit establishing SSL, IPsec and 802.1x connections for network devices is normally a lengthy process. ACE simplifies the process for Platform A solutions-enabled devices in an Active Directory environment, requiring entry of only a limited number of domain control and user identity parameters.

Contactless card authentication support: Badge authentication solutions include contactless card solutions (applications) for basic badge authentication. This option is available when user identity is linked to office security ID badges. The solutions can verify the badge ID and retrieve user information so the Lexmark device can access held print jobs, identify the source of scanned documents, or identify a user for other purposes.

CAC/PIV and SIPR card authentication: The Common Access Card (CAC) and Personal Identity Verification (PIV) authentication solution* provides safe workflow processes for more control over the security of networked Lexmark MFPs in federal government operations. Digital-information-capture functions require strong user authentication to protect against unauthorized access and guard critical data. The same solution also supports SIPR token cards (using a different card interface application) to provide access over the Secret Internet Protocol Router Network.

Secure Content Monitor: Reduce the risks and liabilities associated with security breaches of physical documents. Secure Content Monitor* can simultaneously monitor and audit the information in millions of documents coming from all of your printers and multifunction products, whether printed or scanned, to improve the way your enterprise detects, investigates and deters wrongdoing.

Hard disk security

Some Lexmark printers and multifunction products include internal hard disks to store images of documents that are printed, scanned, faxed, or copied. The internal hard disk also stores data that extends the devices' capabilities and functionality. These devices contain a broad array of carefully engineered features to both enhance the security of data that is stored on the hard disk and help prevent malicious users from gaining access to confidential information.

Hard disk encryption: Hard disks in printers and MFPs can be configured to use encryption. An AES key, up to 256 bits, is internally generated by the printer or MFP and used to encrypt all data on the hard disk. The key is stored non-contiguously on the device, making the contents of the hard disk accessible only on the original printer or MFP. The data on a stolen hard disk would not be accessible even if the hard disk was installed in an identical model of printer or MFP.

Hard disk file wiping: Data written to printer or MFP hard disks for temporary use when printing, scanning, faxing or copying can be erased when the job is done, or after a job held for a user is printed. To ensure the information can never be recovered, Lexmark printer and MFP hard drives both remove the file's reference in the disk directory and erase the actual file on the disk so that no residual data can be read. Depending on the device, hard disk wiping can be configured for manual, automatic or scheduled mode. A multi-pass wipe is also offered, which conforms to NIST/DOD standards.

Complete hard disk erasure: Before a printer or MFP is retired, recycled or otherwise removed from a secure environment, an authorized user can completely erase the hard drive. This includes erasing the forms, fonts, macros or unprinted held jobs that routine hard disk file wiping (above) can leave behind. Options for single or multi-pass erasure are offered, ensuring that no readable data will remain on the disk.

Non-volatile memory wipe: The non-volatile memory wipe provides a tool for erasing all contents stored on the various forms of flash memory contained on the device. This feature is a complete clearing of all settings, solutions, jobs and faxes on the device. It was designed to be utilized when the Lexmark device is to be retired, recycled or otherwise removed from a secure environment.

Out of service wiping: Simplify the process of clearing both a device's disk drive and non-volatile memory data when removing a device from service or removing it from a secure location. Authorized users can do both in one step with the "out of service" wiping command, available from the device's own configuration Menu or from the device's Web page.

Physical lock support: Lexmark 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 the hard disk and other optional components to help prevent tampering or theft.

Standards and certifications

Anyone can say their products are secure. Lexmark seeks and achieves certification for comprehensive industry and government standards.

Common Criteria (NIAP/CCEVS Certification, ISO 15408): Common Criteria provides a framework to validate the security functionality of a computer system. Such third-party validation assures customers that security capabilities protect the device as claimed by the manufacturer.

FIPS: The National Institute of Standards and Technology (NIST) bases requirements and standards for cryptographic modules on FIPS, the Federal Information Processing Standards. Lexmark has completed a FIPS 140-2 Cryptographic Algorithm Validation Program (CAVP) on Lexmark products, an independent validation of the correct implementation of cryptographic algorithms used in our devices.

Find out more

For more information on Lexmark security features, products and services, contact your Lexmark representative or call us at 888-403-2803.

© 2016 Lexmark. All rights reserved.
Lexmark and the Lexmark logo are trademarks of Lexmark International, Inc., registered in the United States and/or other countries.
All other trademarks are the property of their respective owners.

Insight®

Work smarter.

At Insight, we'll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more