Lexmark Security Reference Guide

Lexmark™

When it comes to security, your organization must ensure that it can efficiently manage network devices, defend them from hackers and protect critical information. At Lexmark, we've designed our solutions-capable devices to address the unique security needs of your organization, powered by the industry's most advanced security features.

Secure by Design approach

Securing an enterprise environment is complex and requires a comprehensive understanding of software, hardware, network architecture, the content traveling on the network, human factors, and each organization's security posture and goals. It also requires expert knowledge to translate theoretical security concepts into secure products and services.

Lexmark's systematic, "Secure by Design" approach delivers a critical benefit to our customers: the confidence to cost-effectively run their business, knowing their devices and data are protected every step of the way. Lexmark doesn't treat security as an afterthought or optional feature, but as an integral design and engineering goal, embedded in all our products and services.

Our understanding of network environments and relevant security threats, particularly in relation to printing, gives us the know-how to create unique solutions that secure your data in every possible way—a capability we've proven by working and overcoming security challenges in some of the most highly regulated organizations and industries on earth.

Product design: All Lexmark hardware, software, and firmware are designed using the security principles outlined in our Secure Software Development Lifecycle (SSDL). The process addresses all aspects of security from planning through design and implementation, including quality assurance, release and maintenance. The SSDL offers unmatched protection checkpoints to meet your organization's most stringent security standards.

Supply chain integrity: Through every supply chain step, Lexmark works hard to ensure that our employees, manufacturers and suppliers adhere to the highest standards of compliance, security and social responsibility. This assures the products and parts that leave production are built exactly as specified, yielding an authentic product and eliminating the risk for your organization.

Security features: Our comprehensive approach to security delivers features and functions designed to protect every aspect of your output environment and meets the most stringent industry and government security standards. These are defined and built using the SSDL, and our core security features are integrated into every device we sell.

Industry certifications: Lexmark designs hardware and solutions with the industry's most rigorous specifications. Because of our deep industry experience, we know what certifications are important to each customer based on their unique security profile. Lexmark pursues those certifications and validates every process to ensure sensitive information is protected across the network.

Vulnerability management: At Lexmark, reducing exposure to vulnerabilities is our priority so users can focus on what's important: supporting customers, protecting critical assets and moving their business forward. As defined by our SSDL, Lexmark security experts constantly monitor multiple channels to identify potential security vulnerabilities. If the need arises, our experts react quickly to eliminate exposure to the threat and responsibly disclose the remediation.

Privacy program: Lexmark's privacy program, Privacy at Lexmark (P@L), is a robust organization of over 80 employees at both the corporate and business unit levels. The program's mission is the creation and maintenance of repeatable processes designed to respect and protect the data privacy of our customers and their users, and to comply with global privacy regulations.

Product design

Lexmark hardware, software and firmware are designed using Secure Software Development Lifecycle (SSDL). This process addresses all aspects of security from planning through design and implementation, offering unmatched protection checkpoints.

Core Security Features

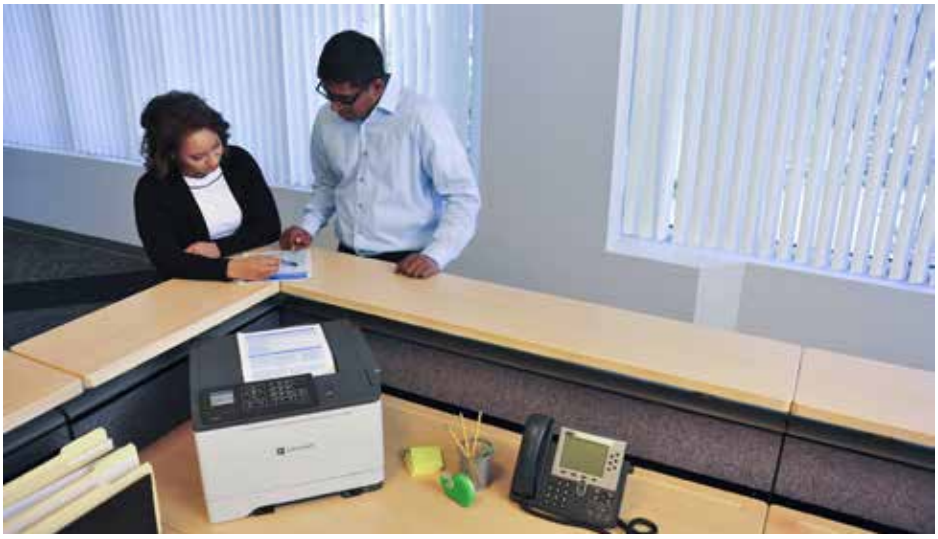
Lexmark's advanced security approach covers a full spectrum of features and functions. Our treatment of malware protections, operating system protections, and firmware updates as related concepts protects every aspect of your output environment and enhances your technology investment.

Secure by Default: Making the right choices in your printer security configuration can be challenging. Starting with Firmware 7, Lexmark turned off many unsecure legacy ports and protocols and turned on disk encryption by default. In addition, the setup wizard makes your out-of-box experience is as easy as it is secure.

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

Secure boot technology: Users can validate that the firmware installed on the printer is genuine Lexmark firmware; if non-genuine firmware is detected, the device will display an error notification.

Continuous verification: Administrators can ensure that firmware has not been tampered with during operation. The code is revalidated every time it is read in from persistent storage.



Secure access features

Most digital security breaches depend on a user pretending to be someone they are not. Lexmark devices are designed to provide unhindered access to the right users while keeping out pretenders. Advanced security features are designed for each product's intended use and flexible options are available to meet your organization's specific requirements.

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 groups of users the right to access specific device functions while restricting other users or groups.

Access controls: Control local and remote access to specific menus, functions and workflows on each device. Users can entirely disable functions like copy, print, fax, scan to email, FTP, held jobs, address book and over 50 other access controls.

Security templates: Device administrators can easily restrict device access by combining group privileges, access controls, and authentication methods into security templates.

Protected USB ports: USB host ports are designed with security in mind and have various mechanisms in place including the ability to disable ports and prevent 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.

Operator panel lock: An MFP can 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 hold: 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 device.

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, 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. Network ports and protocols such as telnet, FTP, SNMP and HTTP plus many others can be explicitly disallowed.

Port authentication: 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.

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.

Fax/network separation: Lexmark offers a variety of MFP devices that provide both network connectivity and fax modem capability. 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 and email addresses exchanged over a TLS/SSL connection are encrypted to preserve the confidentiality and privacy of data.

Document security

Knowing that you need to print documents but still protect the information they contain, Lexmark offers a variety of features and optional products that ensure only authorized users see private output. In addition to fortifying document security, you can also save paper and consumables by printing only what is needed, when it is needed while giving mobile users new printing choices.

Secure print release: Lexmark Print Management allows users to send jobs from any location and pick them up at any print release-configured device on your network. Organizations can improve printing flexibility and protect the confidentiality of information while eliminating the risk and expense of forgotten documents piling up at printers. The entire release process is secured by credentials entered at the device in the form of network user identification or an ID badge, ensuring both security and ease of use.

Confidential Print: By holding jobs on a specific Lexmark printer or MFP until it is released with a PIN, Confidential Print prevents prying eyes from viewing documents in the output bin. Like all forms of print release, organizations only pay for actual documents printed, not the pages someone printed but never picked up.

Lexmark Print Management is available as a premise, cloud or hybrid solution to meet your organization's unique requirements. By moving to the cloud, you can eliminate unsecure printed pages and unpatched print servers.

Secure remote management

To practically manage a fleet of networked print and imaging devices, secure remote management is a must. The device should 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 Markvision Enterprise: To further enhance your organization's security policies, a robust print management software is critical. Markvision Enterprise is a key component of Lexmark's Secure by Design approach and is engineered to ensure optimum security for every device in your network.

With this Markvision Enterprise, you can easily manage device configuration on a fleet of network printers, scalable to thousands of devices. Intuitive features like common configuration, automatic certificate management, forgotten password recovery, custom table views/exports and specified-time firmware updates make it easier than ever to ensure security compliance across the enterprise.

Unlike other print management solutions, Markvision Enterprise manages both device configuration and security policies in a single, easy-to-use tool. And because helping our customers secure their print environment is a key priority, Lexmark offers Markvision software at no cost to your organization.

For organizations looking for the convenience and simplicity of managing their fleet from the cloud, Lexmark offers Cloud Fleet Management. This solution empowers administrators to manage fleets quickly and easily. It reduces the physical infrastructures required and offers the scalability of cloud.

Helping customers secure their print environment is a key priority, which is why Lexmark offers Markvision Enterprise print management software at no cost to your organization.

Device and settings access: 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.

Certificate management: Lexmark printers and MFPs can integrate with a PKI environment using signed certificates for HTTPS, SSL, IPsec and 802.1x authentications.

HTTPS: Lexmark products can use the HTTPS communication protocol to allow web traffic to be encrypted so users can securely perform remote management via the embedded web page.

SNMPv3: 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.

Security solutions

Lexmark laser printers and smart MFPs can run security-related apps to fill special needs like print release*, automatic security certificate enrollment and smart card authentication.

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. Secure print release improves flexibility, protects the confidentiality of documents, saves on printing costs and eliminates the problem of documents piling up at printers. The entire release process is secured by credentials entered at the device in the form of network user identification or ID badges.

Contactless card authentication support: Badge authentication solutions include contactless card solutions for basic 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. The solution also supports SIPR token cards to provide access over the Secret Internet Protocol Router Network.

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

"The Lexmark solution paid for itself in six months and we have eliminated more than 5,000 hours of required staff time by implementing this solution, which is the equivalent of $1.3 million."

Robert Zekanis
Information Management Branch of Directorate of Human Resources

*Optional

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 National Institute of Standards and Technology (NIST) and Department of Defense (DOD) standards.

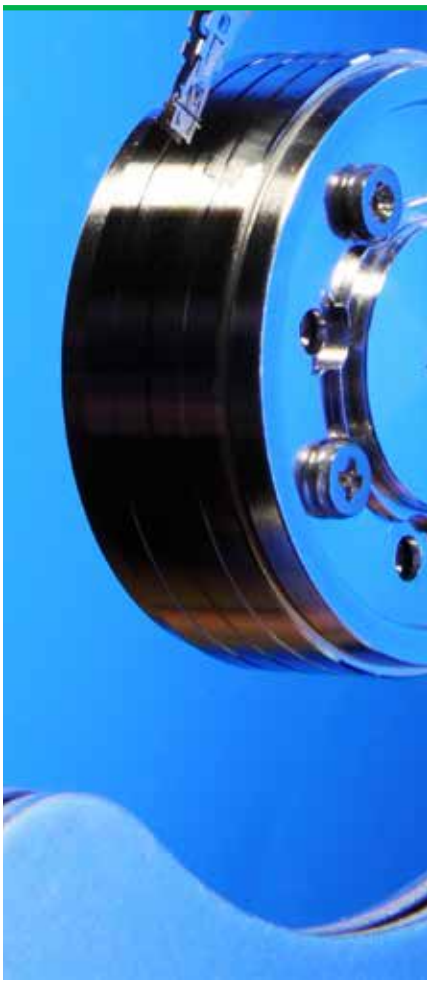
Complete hard disk erasure: Before a printer or MFP is retired, recycled or otherwise removed from a secure environment, an authorized user can completely erase the hard drive. This includes erasing the forms, fonts, macros or unprinted held jobs that routine hard disk file wiping (above) can leave behind. 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.

Out-of-service wiping: Simplify the process of clearing both a device's disk drive and nonvolatile 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 secures the metal cage that houses the hard disk and other optional components to help prevent tampering or theft.

On new devices equipped with hard drives, encryption is on by default which means your organization's data is protected from day one.



Standards and certifications

Anyone can say their products are secure. As part of our comprehensive approach to security, Lexmark seeks and achieves certification for comprehensive industry and government standards.

Common Criteria: Common Criteria (NIAP/CCEVS Certification, ISO 15408) 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.

Federal Information Processing Standards (FIPS): NIST bases requirements and standards for cryptographic modules on FIPS. 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.

ISO 20243: Lexmark is the first imaging manufacturer to receive ISO 20243 certification for supply chain integrity. This standard addresses supply chain security from product development to manufacturing and distribution, and gives customers confidence knowing that Lexmark products are never at risk for counterfeit or tampering.

Other certifications: Additional Lexmark third-party certifications include ISO 27001 for Information Security Management and the UL Cybersecurity Assurance Program (CAP). Lexmark devices are also validated for Information Technology Hardcopy Device and System Security using the 2600-2008 IEEE Standard and compliant with NIST SP 800-193. In addition, Lexmark's Privacy Program was recently named a CS050 Award Winner, which recognizes organizations that demonstrate outstanding business value and thought leadership for security initiatives.

From an analyst perspective, Lexmark product security posture has been recognized by IDC, Quocirca and Keypoint Intelligence. This recognition and our portfolio of certifications helps ensure that your most critical assets and information are protected.