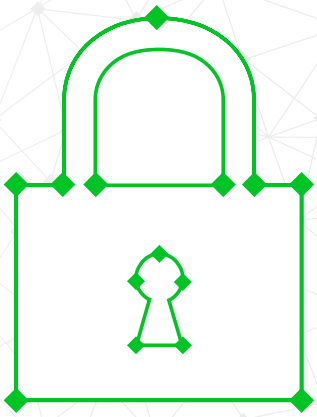
Lexmark™
A Xerox Company



Lexmark Security Reference Guide



When it comes to security, your organization must ensure that it can efficiently manage network printers, defend them from hackers and protect critical information. At Lexmark, we've designed our devices to address the unique security needs of your business, 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 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. In fact, this 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.

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 in the world.

Unlike others, we own all our technology, including hardware, firmware and software. This means that Lexmark's in-house development experts can work with your organization on specific requirements, and react with speed and agility to meet your security output needs.

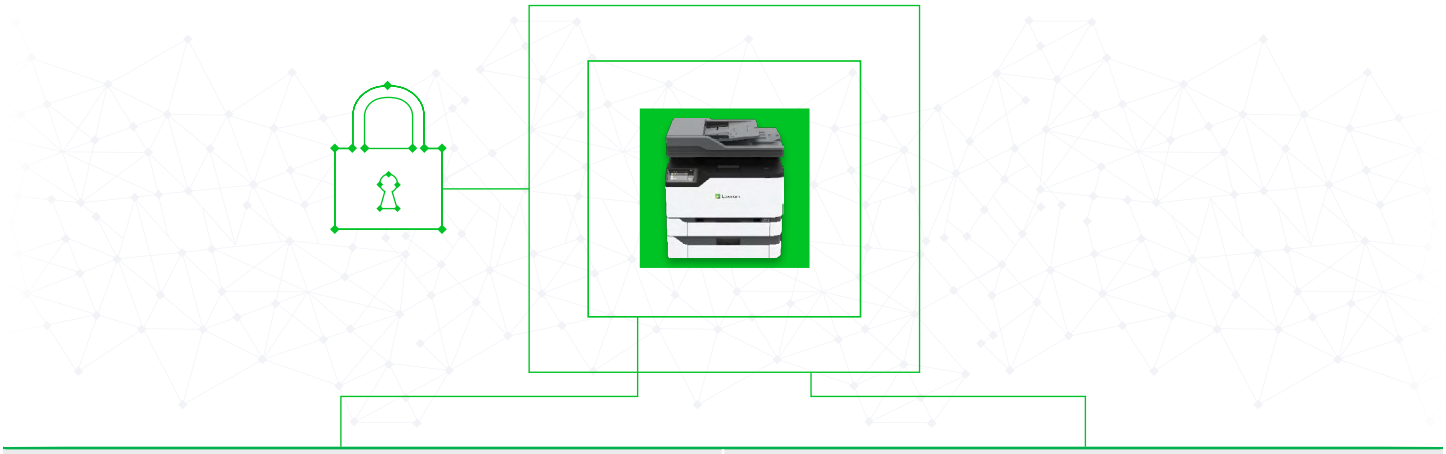


Protect every facet of print security

Lexmark's expertise as an industry leader in document and device security forms the backbone of our technology. Our security profile for Products and Standards combined with our Secure by Design approach helps customers protect their printer fleet with the industry's most comprehensive security offering, right out of the box.

Products

Standards



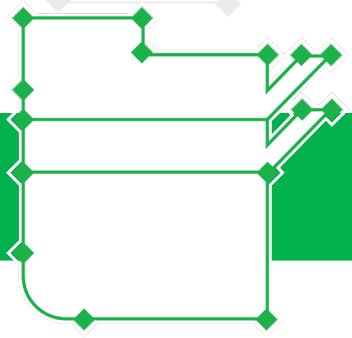
Products

- Secure OS startup and verification
- Trusted Platform Module
- Memory and storage protections
- Firmware protections
- Fax and network separation
- TLS 1.3
- Authentication and Authorization
- Device and settings access
- Secure by Default
- Out of service erase
- Audit logs with secure syslog
- Certificate management
- Secure ports and protocols
- PrintCryption

Standards

- Common Criteria (NIAP/CCEVS Certification, ISO 15408)
- FIPS 140-3 (Encryption)
- SOC2 Type II (Cloud)
- ISO 20243 (Supply Chain)
- ISO 27001 (Information)
- NIST (Standards)

These capabilities form the foundation of a layered, multi-faceted approach to ensure the highest level of device and data security throughout the entire output process. We've built security into every device we produce, from the smallest desktop printers to our largest enterprise MFPs and everything in between. This means you no longer have to choose between a device that is right for your organization, or one that is secure.



Products

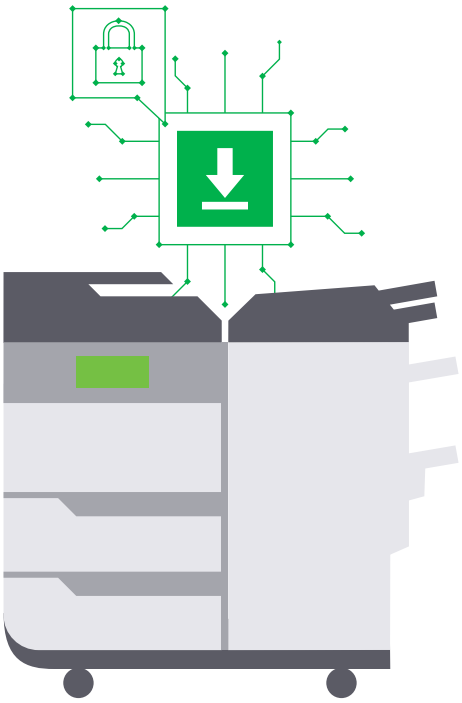
Enhance printer security with industry-leading hardware and firmware



Secure Device

Lexmark printers and MFPs support a robust security offering for endpoint protections and system hardening. Our advanced security capabilities allow users to minimize threats and vulnerabilities while enhancing their technology investment.

- **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.
- **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.



- **Active Directory integration:** Microsoft Active Directory support is provided on solution-enabled Lexmark devices with touchscreen displays. Using Active Directory for the latest generation of Lexmark touchscreen devices is a secure method of authentication and authorization that makes device security management faster and easier for IT resources.
- **Contact and contactless card authentication:** Badge authentication solutions include contact and 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.



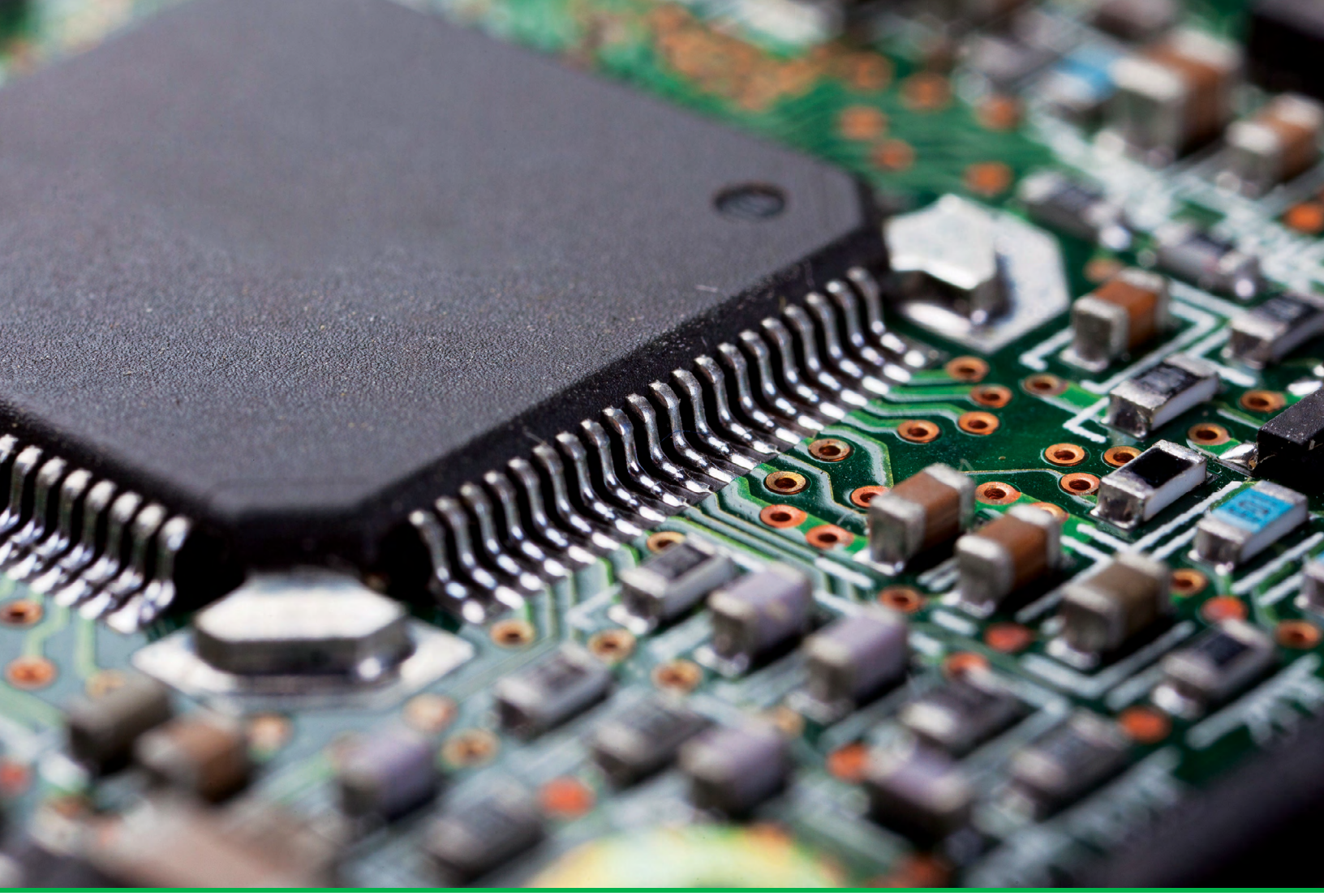
All Lexmark hardware, software and firmware are designed using the security principles outlined in our Secure Software Development Lifecycle (SSDL). The process addresses all aspects of security from planning through design and implementation including quality assurance, release and maintenance, and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



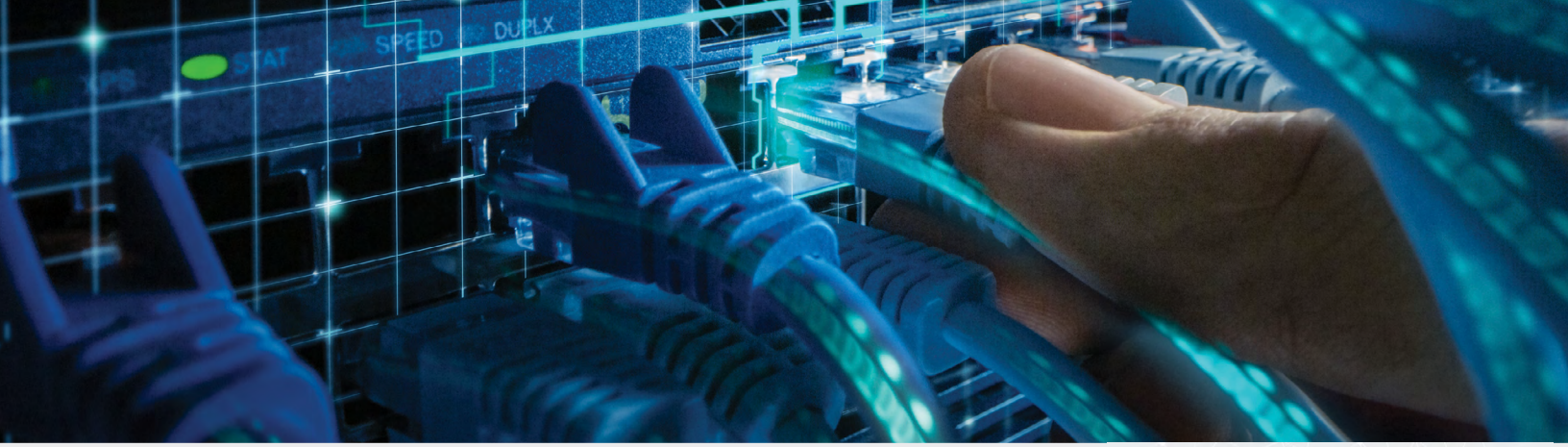
Secure Data

Lexmark devices contain a broad array of carefully engineered features to both enhance the security of data that is stored on the device and help prevent malicious users from gaining access to confidential information.

- **Encrypted storage:** There are various locations to store data in printers and MFPs today, all of which 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. The key is stored non-contiguously on the device, making the contents accessible only on the original printer or MFP. The data on a stolen component would not be accessible even if it 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 disk erasure:** Before a printer or MFP is retired, recycled or otherwise removed from a secure environment, an authorized user can completely erase the drive. This includes erasing the forms, fonts, macros or unprinted held jobs that routine hard disk file wiping 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 erase:** This process simplifies the clearing of data on all storage components 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.



- **Trusted Platform Mode:** Beginning with our 2022 product announcements, we now include a standard Trusted Platform Module (TPM) which delivers authentication, system integrity checks and cryptographic capabilities to create a unique digital system fingerprint. TPM is quickly becoming the industry standard for enterprise hardware security and provides a more secure experience for users by storing hard drive encryption keys on a separate piece of hardware than the data it encrypts with added layers of protection. This hardware also helps make encryption stronger with enhanced random number generation.



Secure Network

From disabling unnecessary features to locking down device interfaces and securing the data they contain, Lexmark devices include a wide range of embedded features to harden a device against attacks.

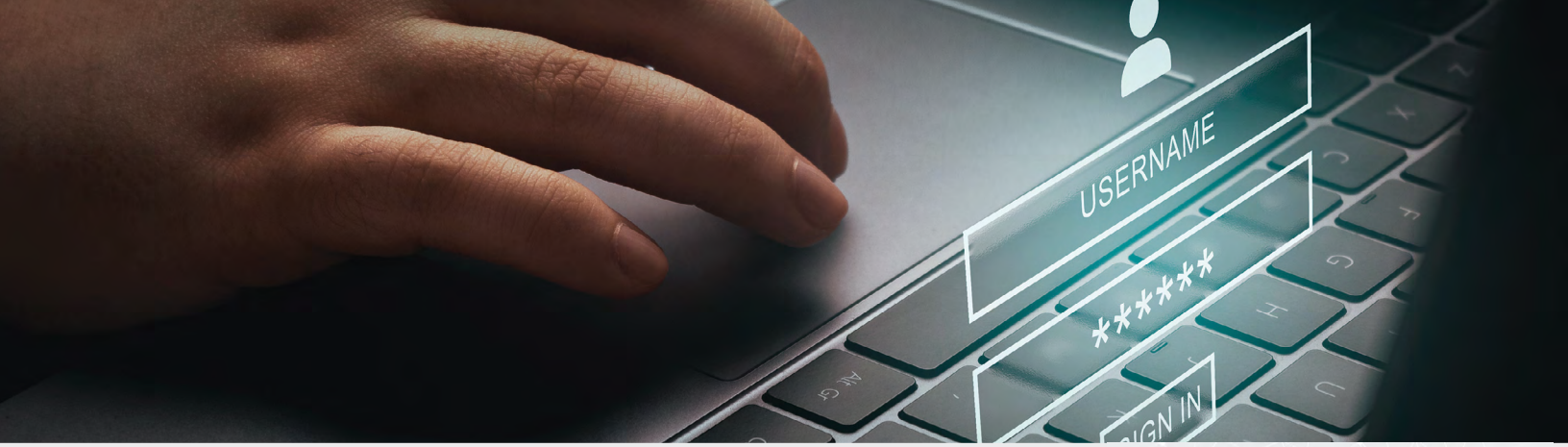
- **TCP connection filtering:** Printers and MFPs can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses which protects the device against unauthorized printing and configuration.
- **Port filtering:** The network ports through which printers and MFPs listen for or transmit network traffic are configurable, allowing a significant degree of control over the device's network activity. Network ports and protocols such as telnet, FTP, SNMP, HTTP and more 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.
- **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.
- **Secure LDAP:** All LDAP traffic to and from Lexmark devices can be secured with TLS. LDAP information such as credentials, names and email addresses exchanged over a TLS connection are encrypted to preserve the confidentiality and privacy of data.



- **Secure by Default:** Making the right choices in your printer security configuration can be challenging. Starting with Firmware 7, when customers opt-in to Secure by Default, there is an option to create an admin account and the device will turn off many unsecure legacy ports and protocols and turn-on disk encryption by default. In addition, the setup wizard makes your out-of-box experience as easy as it is secure.



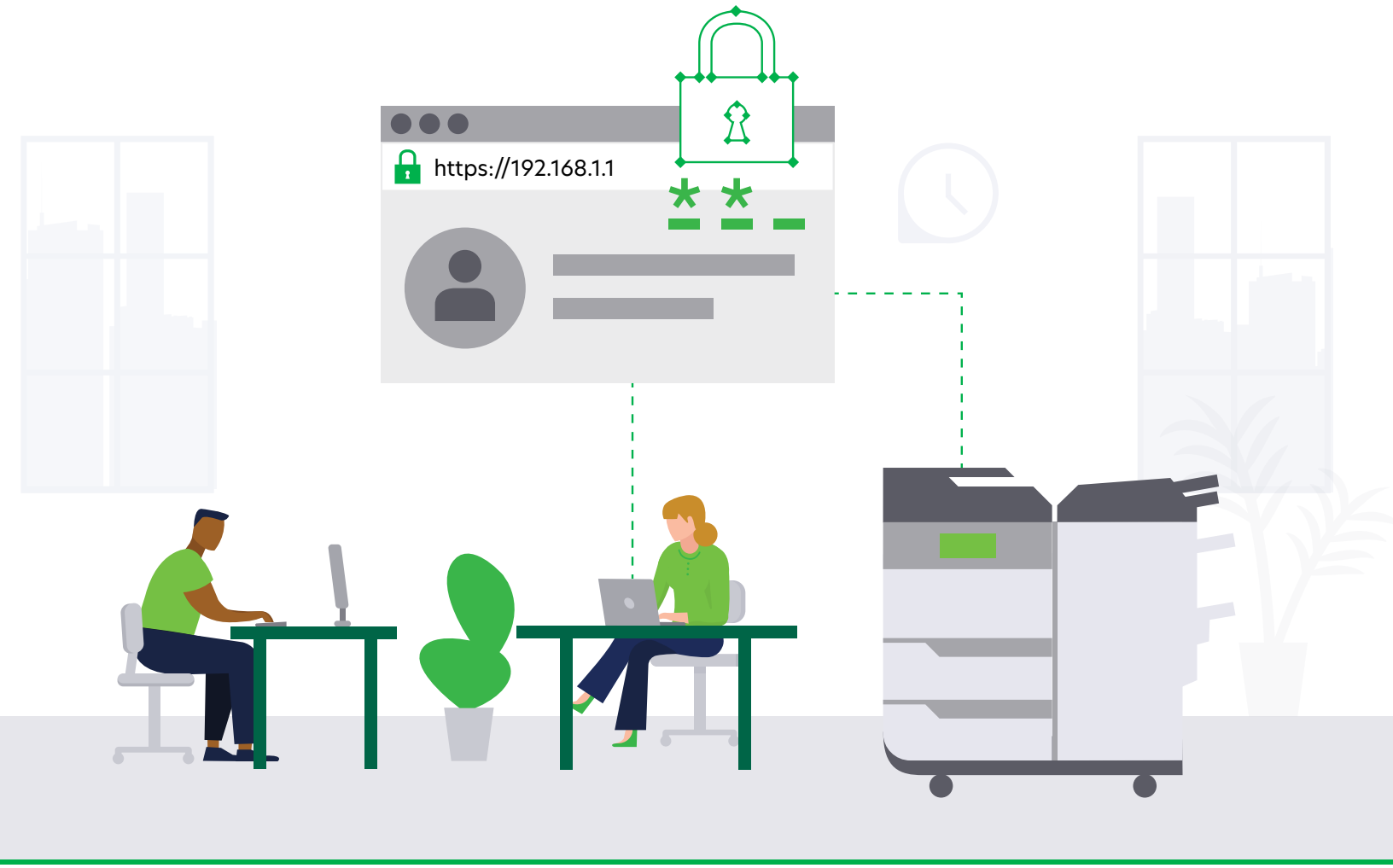
- **Fax and network separation:** Lexmark offers a variety of MFP devices that provide both network connectivity and fax modem capability. To prevent any direct interaction between the modem and network adapter, Lexmark device hardware and firmware keep these mechanisms separate.
- **Incoming fax hold:**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



Secure Remote Management

To meet the demands of effectively managing a fleet of networked printers, Lexmark devices have the remote management security features you need as they permit only authorized personnel to configure the device for network access.

- **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 with secure syslog:** 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.
- **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, Kerberos 5, LDAP, LDAP+GSSAPI, password and PIN.
- **User and group security:** This function allows administrators to grant individual users and groups of users the right to access specific device functions while restricting other users or groups.
- **Access controls:** Administrators can 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. Access to device functions and menus can be set by the selection of a permission for that respective access control.
- **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:** Administrators can prevent unauthorized use of a device by restricting the number of consecutive failed logins and track such events through integrated auditing.



- **Certificate management:** Lexmark printers and MFPs can integrate with a PKI environment using signed certificates for HTTPS, TLS, 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.
- **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.



Standards



Ensure compliance with
third-party certifications



Security Standards

As part of our comprehensive approach to security, Lexmark achieves certifications for comprehensive industry and government standards, and these capabilities have been validated and certified by recognized third-party organizations.

- **ISO 20243 Supply Chain certification:** 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. In fact, Lexmark is the first print vendor with an ISO 20243 supply chain security certification for the entire printing device, including cartridges, supplies and integrated solutions.
- **Common Criteria ISO/1EC 15408:** 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. Devices are validated for Information Technology Hardcopy Device and System Security, using the current protection profile associated with the Common Criteria Evaluation and Validation Scheme (CCEVS).
- **FIPS 140–3 for Cryptography validation:** NIST bases requirements and standards for cryptographic modules on FIPS. Lexmark is leveraging a FIPS 140-3 validated OpenSSL module. FIPS 140-3 (replacing FIPS 140-2) validates the security, reliability, and integrity of cryptographic modules.
- **Third Party Analyst perspective:** From an analyst perspective, Lexmark product security posture has been recognized by IDC, Quocirca and others. This recognition and our portfolio of certifications helps ensure that your organization's assets and data are protected.



Security Governance

The Lexmark Security Governance team is responsible for ensuring safeguards to protect the confidentiality, integrity and availability of data. Lexmark's comprehensive approach to security helps our customers protect sensitive information by delivering highly secure products and services across every industry.

- **SOC 2 Type II for Lexmark Cloud:** Lexmark Cloud Services has achieved and maintains Service Organization Control (SOC) compliance. The latest SOC 2 Type II report is available by request to customers and prospective customers who have an active non-disclosure agreement (NDA). Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles": security, availability, processing integrity, confidentiality and privacy.
- **ISO 27001 information management:** Lexmark has obtained the ISO 27001 certification for its worldwide Managed Print Services, Predictive Services and Cloud Configurations Services. ISO 27001 is an information security management system (ISMS) international standard that provides a comprehensive set of requirements for maintaining confidentiality, integrity and availability of data.
- **Implemented Zero Trust strategy:** The primary concept behind the zero-trust security model is "never trust, always verify," which means that users and devices should not be trusted by default, even if they are connected to a permissioned network. Lexmark understands that organizations are considering zero-trust principles to provide tighter access controls, both inside and outside the network perimeter. With this in mind, securing an enterprise environment is becoming more complex and requires a comprehensive understanding of software, hardware, network architecture and each organization's security goals.
- **Privacy program:** Lexmark's privacy program 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.

For more detailed information, please view the Lexmark Security Whitepaper at https://www.office.xerox.com/latest/SECWP-06U.pdf

© 2026 Lexmark is a Xerox Company., registered in the United States and/or other countries. The Open Group Certification Mark and Open Trusted Technology Provider are trademarks and The Open Group is a registered trademark of The Open Group. To learn more about AICPA, visit www.aicpa.org/soc4so. 03/26 TSK-8685 SECGL-01UA