Lexmark

Secure by Design: Lexmark Print Devices

Security White Paper

March 2026

Contents

Executive overview

To enhance the security of their infrastructure, organizations implement security methodologies and strategies such as Secure Access Service Edge (SASE), defense in depth, and Zero Trust. Proprietary data has become a cornerstone for innovation and is one of an enterprise's most valuable assets. Companies face many challenges when developing security strategies, including inadequate or legacy security practices and effectively managing large fleets of devices.

Lexmark's expertise as an industry leader in document and device security forms the backbone of our strategy. Our comprehensive approach to security covers a full spectrum of features, solutions, software, and services designed to protect every aspect of our customers' output environment. This time-tested, systematic approach gives customers the confidence to efficiently and cost-effectively get the job done, knowing that their devices and data are always protected.

Lexmark's products meet the most stringent industry and government security standards, including Common Criteria and Federal Information Processing Standard (FIPS). Our security ecosystem is designed to overcome the most complex data protection challenges for every business in every industry.

In 2020, Lexmark was the first printer manufacturer to achieve the ISO 20243 certification on an entire printing device, including supplies. ISO 20243 is an accreditation that certifies the supply chain integrity of hardware products, evaluating development practices, supplier management, related IT systems, manufacturing processes, and logistics.

The ever-changing security landscape has led Lexmark to work closely with our customers to help provide advice and solutions to mitigate risks related to their print environment. Lexmark security services ensure that our customers' print devices and security policies are configured according to their specific security goals and industry best practices. Lexmark's dedicated security consultants assess vulnerabilities and risk for print devices (inclusive of firmware, settings, and authentication) and effectiveness of existing print device management strategies.

When configuring Lexmark devices, consider the security posture of an organization. Since no two customers are alike, we seek to provide a consultative approach toward a holistic output strategy that elevates security while enabling business functionality. Combined with our award-winning devices and fleet management tools,

Lexmark's portfolio of security solutions is equipped to enable full-spectrum security protection across various print environments.

26WWM13805

Zero Trust

Understanding the Zero Trust security model and Lexmark's approach

Zero Trust is a security strategy and not a technology. The main concept behind Zero Trust is "never trust, always verify." It means that users and devices cannot be trusted by default, even if they are connected to a permitted network.

Zero Trust is a proactive, integrated approach to security across all layers of the digital estate. It explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats.

Zero Trust is imperative for business, technology, and security teams working to protect complex environments. It is an ongoing journey for security professionals, but getting started begins with simple first steps and continuous iterative improvements.

Zero Trust principles include the following:

- Segmenting and compartmentalizing data
- Ensuring endpoint security
- Not trusting, always verifying
- Least privileged access

Lexmark realizes that organizations are considering Zero Trust principles to provide tighter access controls, both inside and outside the network perimeter. Securing an enterprise environment is becoming more complex. It requires a comprehensive understanding of software, hardware, network architecture, human factors, and each organization's security posture and goals.

Lexmark supports Zero Trust Architectures (ZTA) today with our advanced device management and conformance tools, on-device runtime and firmware protections, and security analysis and analytics services. Our products include features designed to fit our customers' varied security risk profiles. We use capabilities such as core device security, device and data hardening, and security solutions and services.

Depending on the security requirements of your organization, we can also use one of our Software Alliance partners. They include LRS, PaperCut, PrinterLogic, Kofax, innerActiv, and a long list of other partners to further align with your Zero Trust initiatives and strategies.

Lexmark Secure Software Development Lifecycle (SSDL)

Lexmark Secure Software Development Lifecycle (SSDL)

Lexmark is a global technology company that creates enterprise software, hardware, and services. It helps organizations draw deeper value from their business information and serves customers in 170 countries. This section describes Lexmark's process of developing software and hardware products that are more secure and better meet the security requirements of customers.

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.

Lexmark's SSDL process is a series of development and review activities that address various aspects of security that must be considered when writing, testing, and releasing software. This process provides a framework for designing enterprise software and hardware products that are more resilient in the changing security landscape and meet customers' security requirements.

Most SSDL security practices are generally applicable to all Lexmark software and hardware. But Lexmark evaluates each software or hardware product with the most applicable and appropriate security standards for that product or product class. The evaluation is based on factors not limited to target market, product maturity, and target user environment.

For more information, go to Secure Software Development Lifecycle Whitepaper.

Vulnerability management

At Lexmark, reducing exposure to vulnerabilities is our priority so that users can focus on supporting customers, protecting critical assets, and moving their business forward. As defined by our SSDL, Lexmark's security staff and experts monitor multiple channels for the identification of new security vulnerabilities. These channels include internal reviews, customer service, press relations, academic research, and alerts from organizations like NIST National Vulnerability Database and US-Computer Emergency Readiness Team (US-CERT). When the need arises, our experts react quickly to eliminate exposure to the threat and responsibly disclose the remedy.

Vulnerabilities affecting Lexmark's products are addressed through the following process:

1. The vulnerability is analyzed to determine if it affects the product. (Vulnerabilities found in shared systems or third-party code libraries are remediated, depending on the way the code is used in the system.)
2. Lexmark's security staff determines if the exploit mechanism for the vulnerability is possible at Lexmark's implementation.
3. If so, then the security bug is scored using the industry-standard Common Vulnerability Scoring Systems (CVSS).

Note: The severity score published in a technical alert can differ in specific implementations.

4. Internal processes are initiated to log, track, patch, and test the bug fix, and an updated code is provided through a patch process.
5. If the CVSS score warrants it, then Lexmark issues a security advisory for the products affected.

For the latest Lexmark Security Advisories, go to https://support.lexmark.com/alerts.

To submit a potential vulnerability or concern to the team, send an email to securityalerts@lexmark.com. This submission form allows for direct communication with our subject-matter experts. We then follow our standard vulnerability process to assign severity and timelines for resolution.

To receive communications for Security News and Updates, subscribe at

https://www.lexmark.com/en_us/GlobalPreferenceCenter.html.

Importance of firmware updates

This section provides awareness on the importance of keeping firmware current on your Lexmark devices. If the devices are not running the latest version, then the devices can be at risk. Firmware helps to improve the performance, reliability, and security of the device. Developing a firmware update strategy ensures that you are taking advantage of the latest device features, hot fixes, and security fixes to address known vulnerabilities.

What is firmware?

Firmware is a set of instructions that make the hardware work and do what its manufacturer intended it to do. The firmware consists of device features and functions, security, network components, solutions, solution platform, and more.

Why do we need firmware updates?

Firmware is crucial for maintaining functionality and security. Lexmark continually provides updated firmware that is responsible for running the device. It is important for your organization to determine how to handle these critical updates and fixes and develop a firmware update strategy. It is highly discouraged to downgrade firmware, as it could present an opportunity to exploit the device with known vulnerabilities.

Upgrading the firmware can provide the following benefits:

1. Include fixes to known security vulnerabilities.
2. Possible device speed and efficiency improvements.
3. Increase device capabilities by enhancing current features or adding new features to the device.
4. Resolve firmware or hardware issues that you are experiencing.
5. Enhance device compatibility with newly introduced operating systems or software printing applications.

Tools for Updating Firmware

1. MarkvisionTM Enterprise (MVE)
2. Cloud Fleet Management (CFM)
3. Device Deployment Utility (DDU)
4. Embedded Web Server (EWS)

Recommendation

To ensure that your devices are most secure and contain the latest features, Lexmark recommends that you keep your Lexmark devices at the latest firmware level, as provided on https://support.lexmark.com.

Helpful links

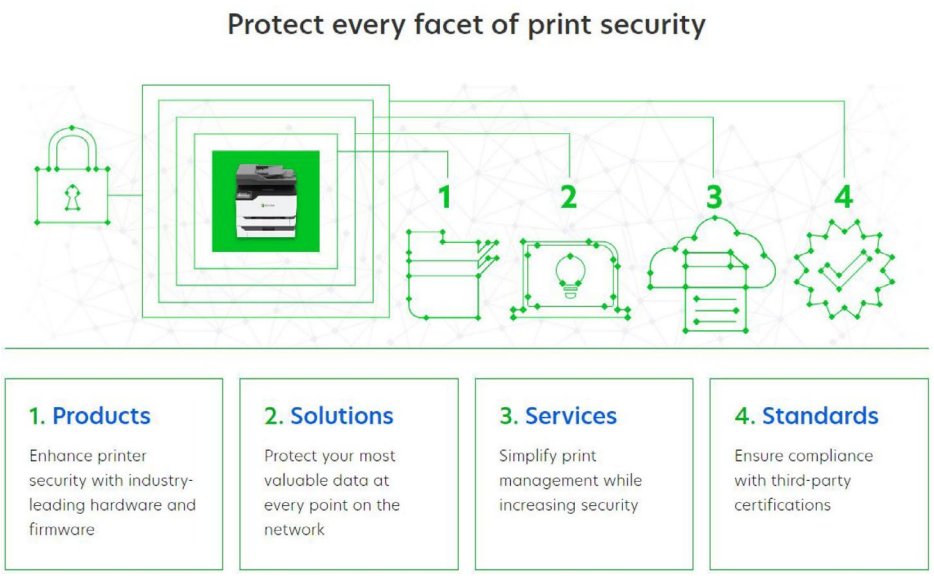
1. For the latest firmware, go to **https://support.lexmark.com**.
2. For the latest Lexmark Security Advisories, go to **https://support.lexmark.com/alerts**.
3. For more information on MVE, go to **https://www.lexmark.com/en_us/solutions/print-solutions/markvision-enterprise.html**.

If you need assistance, please contact the Lexmark Customer Support Center at 1-800-539-6275.

Lexmark Secure by Design Approach

Overview

Lexmark's expertise as an industry leader in document and device security forms the backbone of our technology. Our Secure by Design approach to products, solutions, services, and standards protect customers' fleets with the industry's most comprehensive security offering.



These pillars are the foundation of a layered, multifaceted approach to ensure the highest level of device and data security throughout the entire output process. Lexmark has built security into every device produced, from the smallest desktop printers to the largest enterprise MFP. Customers no longer have to choose between a device that is right for your organization and one that is secure.

Device security, however, is only part of the story. Lexmark's advanced solutions and security services also work together to deliver a complete output security offering that is second to none in the industry.

Products

Overview

Lexmark printers and MFPs support a robust security offering for endpoint protections and system hardening. The advanced security capabilities allow customers to minimize threats and vulnerabilities, while enhancing their technology investment. This protection begins with device features that enhance the security of data stored on the device and help prevent malicious users from accessing confidential information.

Lexmark devices include a wide range of embedded features to harden a device against network-based attacks. These attacks can range from disabling unnecessary services to locking down device ports and interfaces.

26WWM13805

To meet the demands of effectively managing a fleet of networked printers, Lexmark devices have remote management security features at different levels:

- On-device through the Embedded Web Server (EWS)
- Centralized on-premises through Markvision Enterprise
- Distributed through the Cloud Fleet Management (CFM) service

Lexmark Secure by Default

When a device is first powered on, an initial setup wizard (ISW) appears. The ISW gives users the ability to "opt in" to the Lexmark Secure by Default configuration.

Included within FW25, when the ISW appears, there is an option to create an account called "Admin" that is a member of the Admin group is available by default (opt-in) with option to skip the setup (opt-out). This process may vary by country. This account is an internal account (password or PIN) that has all permissions. Beginning with printer firmware (FW7 or later) defines a reasonably secure default configuration that is applied across many areas of the device, including networking, attached devices, access controls, and other key settings.

Restricting access to network ports is a critical method to ensure attack surfaces are reduced on a device. Some rarely used or deprecated services are restricted by default in Lexmark firmware, including the following:

- TCP 21 (FTP)
- TCP 79 (Finger)
- UDP 69 (TFTP)
- TCP 5001 (IPDS)
- TCP 9600 (IPDS)
- TCP 10000 (Telnet)

Additional security settings can be adjusted after completing the account setup in the EWS to customize the device security profile more to meet requirements.

Further information about security setup can be found in the Embedded Web Server Administrator's Guide for the product.

Secure Remote Management

To meet the demands of effectively managing a fleet of networked printers, Lexmark solutions-capable devices have the remote management security features designed to permit access to only authorized personnel to configure the device.

Device and settings access

Changing device settings can be controlled by using function access controls (FACs), authentication, and authorization mechanisms. These controls keep unauthorized users from altering the settings of the device, including security settings.

Lexmark devices support various user authentication and authorization functions. Device administrators can allow individual users and groups to make changes to a device based on the device function and access rights. With this functionality,

individual users and groups can use their network username and password credentials to access devices. The device can determine whether a user has appropriate access based on the rights configured by the network administrator. This level of control applies to network access through the Embedded Web Server and to the configuration of the device through the control panel. For more details on authentication and authorization, see "Authentication and authorization" in the "Secure access" section of this document.

Administrators can also configure Lexmark devices to include a local account that has permission to access the device settings. The local account can be used if the device has limited or no access to the network directory. Passwords can include alphanumeric and other characters to allow for substantial complexity.

Benefits

- Allows access control of device control panel functions
- Specifies who is allowed to configure devices using the Embedded Web Server or control panel
- Provides a secure method of access while the network is down

Details

FACs are settings that can be configured to allow local and remote access to device functions and menus. Each of the device functions and menus can be configured to use one of the following settings:

- No Security (default setting)
- Disabled (available if the function can be disabled).
- Restricted (through the authentication and authorization mechanism specified by a device administrator)

The primary means of device access by users and administrators must be network user accounts (on a corporate directory server) or local user accounts (on the device). By requiring users and administrators to provide credentials for authentication, administrators can configure a device to determine access based on user and group needs. This access is done through a combination of FAC, authentication, and authorization. For more information, see **"Authentication and Authorization" on page 26**.

Audit Logging

When you select Security Audit Log from the Security menu, Lexmark devices can track security-related events and device-setting changes. These actions can be exported to detailed logs that describe system user or activity events. The event-tracking feature proactively tracks and identifies potential risks and may be integrated with your intrusion-detection system for real-time tracking.

Lexmark devices are configured to export the Security Audit Log information to a SIEM (Security Information and Event Management) using industry standard syslog protocols, such as RFC 5424 and RFC 3164. The transmission is encrypted when stunnel is selected.

Benefits

- Tracks device behavior and activities

26WWM13805

- Identifies authenticated users, logging their activities

Details

The security-related events that are tracked are system-related events, setting changes, authentication and authorization events, disk-wiping events, and real-time clock changes. Events that are logged include the following:

- IP address changes
- Logging behavior changes, such as not being able to send the logs to specific destinations or logging settings are changed.
- Jobs started, canceled, or completed
- Setting modifications of the embedded solutions' FAC
- Authentication or authorization success or failure events, including record of user identity
- Security reset by jumper changes
- Reset to factory defaults for settings, FACs, and other device options
- Device settings modifications
- Creation, modification, or deletion of authorization and authentication settings
- Kerberos file changes
- Authorization sessions created or modified
- Active Directory join or unjoin
- Certificates (device and certificate authority) added or removed
- Disk encryption, format, and wiping
- IP Security (IPsec) connection failures
- Time-changed events
- Scan process events
- Embedded Solutions Framework (eSF) application events

Note: Events can also be logged by eSF applications. Generated logs can be stored in the following ways:

- Stored internally in the device
- Sent to a remote syslog server in real time
- E-mailed to administrators
- Exported through the device web page

Logs can also be digitally signed for security.

Digitally signed firmware updates

Overview

Lexmark devices provide a download mechanism that enables firmware updates. It is a common feature among Lexmark products that is useful for receiving feature upgrades and issue resolutions. However, it is important that these firmware updates are carefully controlled to avoid any unintended impacts to device availability or security.

Benefits

- MFP capabilities can be maintained and extended through the application of authorized firmware updates.
- Unauthorized firmware packages and applications cannot be added to the MFP. If the code is not built and signed by Lexmark, then the MFP rejects and discards the package.

Details

Lexmark devices inspect all downloaded firmware packages for several required attributes before the firmware is adopted and executed. The firmware must be packaged appropriately at Lexmark's proprietary format. The packages must be encrypted using a private key that is known only to Lexmark and is embedded securely in all devices. Also, all firmware packages must be digitally signed using Lexmark's authenticated 2048-bit RSA signatures. If the signatures are not valid or if the system determines that the firmware has been changed since the signatures were applied, then the firmware is discarded.

Lexmark's device management tools enable firmware updates to be transmitted over the network to perform fleet-wide upgrades simultaneously. This process can be automated and scheduled, and the process does not require someone to be present at each device. For security, the ability to perform this update over the network can be limited with access control restrictions to authorized administrators. Devices receive the code, validate

it, adopt it, and restart automatically. The process takes just a few minutes, and all the devices are available for use immediately after completion.

Lexmark solutions-capable devices (models with touch-screen displays) support custom applications through an embedded platform called the Embedded Solutions Framework, or eSF. These applications must also be digitally signed by Lexmark before being adopted, preventing users from installing unauthorized applications on Lexmark devices.

Certificate management

Managing certificates

Certificates are used to provide secure TLS, IPsec, or 802.1x connections and to identify other devices on the network securely. Lexmark printers can also use certificates for LDAP over TLS authentication and address book lookups.

Certificate authorities (CA) are trusted entities that authenticate and validate the identity of users, computers, network devices, websites, and organizations by issuing a digitally signed certificate. The digitally signed certificate serves as a credential to validate the identity of the entity during secure communications. This setup allows other participating parties to verify and trust the transaction. Lexmark devices ship with a self-signed certificate that identifies the device on the network and provides some transactional security. However, relying parties cannot verify and trust the device fully until a trusted CA has issued a signed certificate to the device.

Configuring printer certificate settings

1. From the Embedded Web Server, click Settings > Security > Certificate Management.
2. From the Device Certificates section, click Configure Certificate Defaults.
3. Configure the settings.
   - **Friendly Name**—Type a unique name for the certificate.
   - **Common Name**—Type the name for the printer.

   Note: If you want to use the printer host name, then leave this field blank.
   - **Organization Name**—Type the name of the company or organization issuing the certificate.
   - **Unit Name**—Type the name of the unit within the company or organization issuing the certificate.
   - **Country/Region**—Type the country or region where the company or organization issuing the certificate is located.
   - **Province Name**—Type the name of the province or state where the company or organization issuing the certificate is located.
   - **City Name**—Type the name of the city where the company or organization issuing the certificate is located.
   - **Subject Alternate Name**—Type the alternate name and prefix that conforms to RFC 2459. For example, type an IP address using the format IP:1.2.3.4, or a DNS address using the format DNS:ldap.company.com.

   Note: If your printer is using an IPv4 address, then leave this field blank.
4. Click **Save**.

Creating a printer certificate

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. From the Device Certificates section, click **Generate.**
3. Configure the settings.
4. Click **Generate** or **Generate and Download.**

HTTPS

The most common means to configure networked devices remotely, including Lexmark MFPs, is through the device web interface, or Embedded Web Server (EWS). You can configure device settings by pointing a browser to its IP address or host name and providing the proper credentials. However, browsers and the HTTP traffic associated with them are not inherently secure. An intruder can intercept the network traffic used in the web session and determine the user's credentials. To address this concern, Lexmark devices support HTTPS.

Use of HTTPS is optional but strongly recommended. For environments with strict security requirements, Lexmark devices support redirecting requests from an HTTP (TCP 80) to a secure (TCP 443) connection when accessing the EWS.

Benefits

- Ease of use in establishing a connection for the end user. Point the browser to "https://" instead of "http://," and the device and browser automatically processes the rest. HTTPS and TLS are widely used standards.
- Encryption of all data exchanged through the browser, including passwords and any other settings that are set or viewed.
- Integration with preexisting CA or public key infrastructure (PKI) environments. The device certificate that protects EWS traffic can be signed by an enterprise CA.

Details

Lexmark devices include an Embedded Web Server. When a browser is pointed to a device IP address with the "https://" prefix, the device and the client system negotiate a TLS connection. This action involves the device passing its X.509 certificate to the client system to establish its identity. Because the device certificate is self-signed by default, the client typically presents a warning to the user, depending on the settings of the web browser. The client system can choose to trust the self-signed certificate and thereafter does not receive further warnings.

Alternatively, the device certificate can be signed by a CA that is external or internal to the customer's environment. The EWS includes a certificate management page that facilitates this process. Replacing the self-signed certificate with a CA-signed certificate avoids the warnings associated with the HTTPS session. The HTTPS session is built on a TLS connection in which all exchanged data is encrypted. It protects the contents of the session against eavesdropping and enables secure remote management of the device.

Notes:

- Device EWS access can be restricted to HTTPS only by turning off the HTTP port, leaving only the HTTPS port (443) active.
- Forced HTTPS redirection requires that both TCP port 80 and TCP port 443 are enabled in the TCP/IP Port Access menu.

SNMPv3

Overview

Simple Network Management Protocol (SNMP) provides another means to configure Lexmark devices remotely. SNMP can be used to both view and modify device settings. As a result, controlling its use and protecting associated network traffic are relevant concerns. Lexmark devices support the latest version of SNMP (SNMPv3), which includes authentication and data encryption capabilities. SNMPv1 and v2 are also supported for backward compatibility but are insecure and not recommended.

Benefits

With support for SNMPv3, Lexmark devices can be managed securely with standard SNMP console applications. There are two important elements to the security provided by SNMPv3:

- With authentication, authorized systems can see and manage devices through SNMPv3 while shutting out unauthorized systems.
- Encrypting SNMPv3 traffic protects potentially sensitive device operations data from being intercepted over the network.

Details

Lexmark solutions-capable devices support SNMPv3. This protocol features extensive security capabilities, including authentication and data encryption for performing secure remote management of a device. SNMPv1 and SNMPv2 are also supported.

Using the authentication features of SNMPv3, Lexmark devices can refuse SNMPv3 traffic unless the requests include valid credential hashes in either MD5 or SHA1 format. SNMPv3 access to read or change settings can also be segregated by using read-only or read-write accounts, both supported by Lexmark devices. SNMPv3 data privacy is provided by using the Data Encryption Standard (DES) or Advanced Encryption Standard (AES) with 128, 192, or 256 encryption algorithms to encrypt traffic. Like other mechanisms for managing devices, SNMP can be disabled. If the protocol is not used in a particular environment, then it must be turned off entirely.

Note: To use SNMPv3 securely, Lexmark recommends disabling SNMPv1 and v2. You need to set a user credential, and select the minimum authentication level settings Authentication and Privacy.

Secure password reset

Overview

With the security password reset feature, you can recover a device that is locked down using one of the authentication mechanisms of the device. This feature can also be used if the administrator's password is lost or forgotten or the device loses network connectivity. You can use a cable lock to ensure that the device is not reset maliciously.

Benefits

Provides a two-way method to recover a device for the following scenarios:

- If a local password is lost or forgotten
- If the device cannot communicate with the network.

Details

The security reset feature requires the device administrator to set up the action of the security reset jumper in the Miscellaneous > Security menu. There are two options that can be set on the security reset jumper:

- No Effect—If the security jumper is reset, then there is no change to the security of the device.
- Enable "Guest" Access—The default setting. It resets all FACs in the Security menu to No Security. No data is wiped, and any existing settings and credentials are retained.

If all users are locked out of a device, then the device administrator can do the following:

- Turn off the device.
- Access the physical controller board inside the device.
- Move the security reset jumper over to cover the middle and unexposed prongs to trigger the configured action at startup.

Secure Network Interfaces

Hardening a networked device is a powerful way to secure its network interfaces from malicious users. This includes blocking unnecessary features and functions, locking down any ports that remain and securing the data hosted by the device. Lexmark devices include a range of features embedded in the firmware to help you harden the device.

TCP connection filtering

Overview

Solutions-capable devices can be configured to allow TCP connections only from a specified list of IP addresses, also known as whitelisting. This mechanism blocks all TCP connections from other addresses, protecting the device against unauthorized printing and configuration. Lexmark devices support connection filtering with the Restricted Server List field.

Benefits

- Approved systems, such as print servers and administrative workstations, are allowed to make connections to your device. This security feature allows normal and approved functions such as printing, routine monitoring, and maintenance.
- All network interactions that involve TCP/IP connections can be controlled to increase security. The following types of connections rely on TCP/IP:
  - HTTP and HTTPS browser connections
  - FTP
  - Printing through the Line Printer Remote/Line Printer Daemon (LPR/LPD) protocol or through the Windows print subsystem
- End-user systems can be omitted from the list, which prohibits them from connecting to the device through a web browser, FTP, or direct-print connection.

Details

The restricted server list allows up to 10 IP addresses or subnets to be specified. The device normally responds to any address in the list and rejects connection requests from any address that is not on the list. The restricted server list does not affect UDP or ICMP traffic. Hence, connectionless interactions and availability requests, such as PING, are allowed from any address.

Port filtering

Overview

Gain more control over your Lexmark device connectivity with port filtering to filter out traffic on specific network ports. Protocols such as FTP, HTTP, SNMP, and many others can be disabled.

Port filtering on Lexmark devices acts as a granular filter that disables network ports individually. With port filtering, devices can be configured to comply with virtually any network protocol restrictions.

Benefits

- Increased security—Provides granular and authoritative control over protocols the device processes or ignores.
- Cleaner port scans—By shutting down unneeded ports, the port scans do not report phantom vulnerabilities that must be tracked down and understood.

Details

The device allows each of the following TCP and UDP ports to be individually opened or closed:

- TCP 21 (FTP)
- UDP 69 (TFTP)
- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 137 (WINS)
- UDP 161 (SNMP)
- UDP 162 (SNMP traps)
- TCP 515 (LPR/LPD)
- TCP 631 (IPP)
- TCP 5001 (IPDS)
- UDP 5353 (mDNS)
- TCP 9100 (Raw Print)
- UDP 9200 (Discovery)
- UDP 9300/UDP 9301/UDP 9302 (NPAP)
- TCP 9400 (Enhanced Print Port)
- TCP 9500/TCP 9501 (NPAP)
- TCP 9600
- ThinPrint
- UDP 3702/TCP 65001 (WS-Discovery)
- TCP 65002 (WSD Print Service)
- TCP 65003 (WS-Eventing)
- TCP 65004 (WSD Scan Service)
- TCP 9198 (PrintCryptionTM)

Note: These settings are based on Lexmark firmware release version 23.

When a port is closed, a device does not generate or respond to traffic on the specified port. The device stops responding, even if the corresponding network service is enabled. It is good practice to close any ports that you do not plan to use under normal operation to reduce your potential attack surface.

Lexmark has removed any configuration capabilities for Telnet due to security risks associated with the protocol. If a customer requires Telnet (usually for legacy applications or utilities), Lexmark enables the protocol on solutions-capable devices through a special-issue license. The license is locked to a specific device to prevent malicious users from deploying it widely and enabling Telnet on all Lexmark devices in a fleet.

Lexmark devices have flood-protection capabilities to help limit device downtime associated with Denial-of-Service (DoS) attacks. If the device determines that it is being attacked, the device conducts a soft reset on its network interface. Then it tries to reestablish normal network operations.

Note: Available ports may vary by model and firmware version.

802.1x

Overview

Virtually all business environments require authenticating with the network. Authentication is required before a user can send or receive email, browse the web, or initiate other tasks. Increasingly, it is important to require devices, such as laptops or MFP, to be authenticated before they can access networks. The protocol for this authentication is 802.1x, and Lexmark devices support this capability out of the box.

Benefits

- Helps the Lexmark device to authenticate and increase its trust level to network users and services
- Compatible with almost any 802.1x authentication environment
- Supports 802.1x with Lexmark's optional wireless network adapter, which provides secure wireless networking capabilities

Details

With 802.1x, devices can join wired and wireless networks that require enterprise authentication. WPA-Enterprise security is also supported when using 802.1x port authentication with the Wi-Fi Protected Access (WPA) feature of an optional wireless print server.

Support for 802.1x is often applied specifically to wireless device security. To provide flexibility across many different deployment scenarios, Lexmark's implementation of 802.1x supports both wired and wireless environments.

The following network authentication methods are supported:

- LEAP
- PEAP
- EAP-MD5
- EAP-MSCHAPv2
- EAP-TLS
- EAP-TTLS with the following authentication methods:
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - PAP

Lexmark devices can be configured to include or exclude each of these protocols in the 802.1x protocol negotiation. Device login, password credentials, and device certificates are supported.

IPsec

Overview

IPsec is supported on Lexmark devices. This network protocol allows the device to establish a secure connection to other network nodes, such as print servers and management workstations. IPsec is available in conventional operating systems, such as Windows and Linux.

Application of IPsec between the device and a workstation or server secures the traffic between these systems with strong encryption.

Benefits

- Confidentiality of traffic between the device and other configured IPsec endpoints is ensured. This protection is extended to protocols that are not inherently secure on their own, such as SNMPv1/2c and FTP.
- Device management and monitoring of traffic can be protected.

IPsec can be used to protect any IP-based network traffic between Lexmark devices and hosts, no matter what operation is performed by that traffic.

Details

IPsec safely sends information to your solutions-capable printers and MFPs by securing all network traffic to and from Lexmark devices with encryption and authentication. You can also protect the contents of jobs that are scanned to any configured destination, including servers running Lexmark Document Distributor, email, and network storage.

Lexmark devices support IPsec with preshared keys and certificates, and these modes can be used simultaneously. In preshared key mode, printers and MFPs can be configured to establish a secure IPsec connection with up to seven other host systems.

In certificate mode, Lexmark devices can be configured to establish a secure IPsec connection with up to five other systems or subnets. In this configuration, printers and MFPs can exchange data securely with various systems, and the process can be integrated with a PKI or CA infrastructure. The use of certificates provides a scalable solution, without the burden of configuring or managing keys or passphrases.

Lexmark devices can store and apply two certificates for use with IPsec. Each device 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 available through the device EWS. With this certificate generation, other systems in the CA environment validate the identity of a device. The Lexmark device can also store the certificate as a trusted root CA certificate, letting it validate the identity of other systems in the CA environment.

Authenticated Network Time Protocol

Overview

Network Time Protocol (NTP) provides devices with a common time source to keep them synchronized with the correct date and time. NTP enables you to use any network authentication method that requires accurate time between a client and server. To ensure that the date and time are delivered only from an approved time source, NTP with optional authentication is supported.

Benefits

Authenticated NTP provides the capability for devices on the network to obtain their time from an authenticated, secured source.

Details

Lexmark devices support the use of authenticated NTP, which is used for clock synchronization of various devices on the network.

Authenticated NTP uses keyed-MD5 hashes to validate the integrity of time stamps received from the time server. These keys are agreed on in advance between the printer and the time server. If a time update comes to the printer from the server without the correct cryptographic hash, then the printer ignores the message.

Fax and network separation

Overview

A common question about networked MFPs is "Are they exposed to intruders with the presence of a fax modem?" The concern is that an intruder can dial in to the MFP through the fax modem. The intruder can also manipulate the device or access its network.

The reality is there is no exposure through a fax modem or network access on Lexmark MFPs. With the fax modem on Lexmark devices, only the exchange of facsimile images is possible. There is no path by which the fax modem connection can interact with or control the MFP network interface. And there is no facility to configure the MFP settings through the fax modem connection.

Lexmark fax modem connections are restricted to Facsimile Class 1 mode. Data transferred over the modem is limited to facsimile image data only. This connection is not the same as on a laptop or other device where an arbitrary network connection can be established through the modem. That connection enables bidirectional communication and data flow.

Network protocols are not supported through the fax modem. There is no support for exchanging TCP/IP traffic of any sort, including FTP, HTTP, SNMP, or any other form of network packet. Also, there is no support for modifying an MFP configuration through the fax modem connection. Settings cannot be viewed or changed, and there is no access to the MFP file system through the fax connection.

Benefits

- Incoming fax images can be printed as hard copy or routed to a predefined email, FTP, or workflow destination. This action does not undermine the device security because 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.
- Incoming faxes can be redirected to an alternate fax machine. This redirection can be useful when an office is temporarily closed, as it allows forwarding of incoming faxes to an alternate device that is regularly monitored.

Details

The following are several reasons why the presence of a fax modem on a Lexmark device with a network adapter does not pose a security risk:

- Controlling the device through the phone connection is not supported. You cannot dial in to the device and interact with it through FTP, HTTP, or similar mechanisms.
- The modem and network adapter hardware are on separate cards and cannot communicate directly with one another. This separation prevents data from moving between the two channels.
- The modem configuration is limited and controlled by the MFP firmware. The MFP firmware does not allow arbitrary data to be exchanged over the fax modem—only facsimile data representing page images can be exchanged.
- The avenues by which the MFP firmware can be updated are secured, and fax is not a supported firmware deployment method.

No control of the device through phone lines

Many devices that support an analog phone modem can be controlled remotely through the phone line. On such devices, you can call the device and interact with it—turn it on or off, change its settings, and so on.

Typically, these actions are managed through outdated plain-text protocols such as Telnet. However, the presence of an analog phone modem does not automatically guarantee the availability of any such mechanism.

Lexmark products do not include or allow this kind of control.

The modem and internal network adapter are separate by design

Lexmark MFP uses a third-party fax chip to handle analog-to-digital processing, but the Lexmark firmware handles the rest of the fax modem process. The internal network adapter functionality of the device and its modem capabilities are implemented on separate circuit boards. Also, the Lexmark firmware is engineered to prevent direct interaction between the fax and network components.

The modem is configured for fax only

Control of the fax functionality is incorporated directly into the Lexmark firmware. Lexmark firmware directly controls the fax chip that sends and receives data over the phone line. The modem chip is in a mode that is even more restrictive than Class 1 mode. And this chip relies on the Lexmark firmware for the composition and transmission of fax data. The firmware explicitly blocks the transmission of frames in data mode and allows only sending and receiving facsimile jobs.

No support for the PostScript® (PS) emulation fax mechanism

Some fax devices employ a mechanism known as PS emulation fax or file transfer. When two devices supporting PS emulation fax connect through an analog phone

session, they can transmit a print job in its original PS emulation format. This setup is faster and produces higher-quality output than converting the job to a bitmap before transmission. However, this setup poses risks to devices that are permitted to accept nonimage fax data. The print job itself can include malicious instructions, and any support for executing nonimage data can leave a device vulnerable. For these reasons, the PS fax capability is not supported on Lexmark MFP.

Phone lines do not provide a way to update firmware

Because the modem can be modified through its firmware, and phone lines are often connected to the outside world, the concern over device compromise is valid. The design of the Lexmark firmware and fax modem operation, however, is to accept only fax frames—frames that contain image data. When these frames are combined, they are assembled and wrapped in PS emulation commands. These frames are submitted to the MFP interpreter as image data. No other data path is available, and there is no way for data coming through the fax to be treated as anything but a fax image. If the data that is received does not represent an image, then the data is purged as an invalid PS emulation job. There is no avenue for modified firmware (or any sort of executable code) to be packaged as a fax job and installed on a Lexmark device.

Secure Access

Network scans and printed documents that routinely contain sensitive information—such as financial data, customer identification, and account information—are often overlooked in MFP security. Lexmark devices include standard features that can substantially reduce security risks. The risks are reduced by ensuring that only authorized users have access to the stored data.

Two levels of device security

The following are levels of security that are supported based on the product generation and control panel type:

- Simple level—Supports only internal-device authentication and authorization methods.
- Advanced level—Supports internal and external authentication and authorization, and restriction capabilities for managing and accessing functions and solutions.

Advanced security is supported on devices that support the installation of solutions or applications to the device. In general, if the device supports a touch-screen display, then the security level for that device is advanced.

Advanced-level security devices support a wide range of local and network authentication and authorization methods. For local authentication, PIN, passwords, and username-password combinations for locally defined users are supported. For network authentication, LDAP, LDAP+GSSAPI, Kerberos, and Active Directory are supported.

Authorization can be specified individually or by groups (either local or network). Devices that support advanced-level security can run installed solutions, allowing the usage of card readers to provide advanced two-factor authentication.

Simple security, found on previous-generation devices, uses the following:

- A single PIN to restrict user access to the control panel of the device. PIN access for the control panel is specified because text entry is generally difficult on the panels for these devices.
- A single EWS password to restrict administrator access to the device. EWS access supports passwords because there are no device panel restrictions.

Authentication and Authorization

When you select a function, such as Scan to E-mail, the MFP can require you to authenticate yourself before proceeding. This limits device access to valid users only and enables the MFP to identify who is performing the function.

Using function access controls (FAC) or permissions, Lexmark devices support granular authorization to requested functions. This feature allows device administrators to grant individual users and appropriate groups the right to access a particular device function. It also restricts other users or groups from using the same functions. With this capability, individual users or group members can use their network directory or local device credentials (PIN, username, and password) to authenticate. Network directory authentication methods support communicating securely with TLS and are compatible with Active Directory and other directory-server platforms using LDAP. The device can determine whether the user has access to the appropriate functions based on the access rights configured by the device administrator. This level of control applies to network access through the device's web server, and to the configuration and use of the device through the touch-screen interface.

An important aspect of authentication and authorization is that if the device is connected to a directory server, then the users can enter their company-issued username and password. Users do not need to maintain a special set of credentials to use a Lexmark device. Instead, the device makes use of the corporate directory to validate user credentials against the standard, centralized database.

Benefits

The benefits of user authentication and authorization are the following:

- Securing an MFP by limiting who can use its control panel to access functions such as Copy, Color Copy or Scan to Network.
- The identity of a user accessing the device is always known. This statement also applies to on-device services such as Scan to Email, where anonymous email is avoided by inserting the identity of the authenticated user.
- With network authentication, logging in is a familiar process for users by using the same credentials as their workstation or laptop. This keeps the process simple and intuitive.
- Faxes sent with network-fax servers can automatically send an email confirmation of the fax to the sender's email, because the MFP recognizes who is sending the fax.

26WWM13805

Details

The process of authenticating users is flexible. Lexmark devices can use various internal authentication mechanisms and network directory authentication mechanisms and protocols to validate user credentials. Lexmark devices can be set up to use internal device accounts, device passwords, device PIN, LDAP (with or without TLS), Kerberos, and LDAP+GSSAP for authenticating users.

Support for a wide array of authentication protocols means that the device user authentication function is compatible with various network environments, including Microsoft Active Directory, Novell eDirectory, and other directory systems that support LDAP. Secure user authentication protocols, such as LDAP with TLS, Kerberos, and LDAP+GSSAPI are supported to protect users' credentials during the authentication process.

The device manages authentication and authorization with one or more of the following methods:

- PIN or Panel PIN Protect
- Password or Web Page Password Protect
- Internal accounts
- LDAP
- LDAP+GSSAPI
- Kerberos 5 (used only with LDAP+GSSAPI)
- Active Directory

To provide low-level security, you can use either basic PIN or Password methods to limit access to a printer—or specific functions of a printer—to anyone who knows the correct credential. This type of security might be appropriate if a printer is located in the lobby or other public areas of a business so that only the employees who know the password or PIN can use the printer. Because anyone who enters the correct password or PIN

receives the same privileges and users cannot be individually identified, passwords and PINs are considered less secure than other credential types that require that identify the user by local account or network-based login ID.

Access controls

Access controls limit availability of functions, applications, and printer management to only authorized users.

Note: Some access controls are available only in some printer models.

Default device settings do not contain any authentication, which means that everyone has unrestricted access to the Embedded Web Server. The initial setup wizard provides administrators the option to configure authentication during device setup.

When the administrator selects Secure by Default during the initial setup, certain administrative menus and device management access controls are excluded from the Public permissions section. For more details, see **"Lexmark Secure by Default" on page 11.**

You can manage access to device functions and menus by selecting a permission for the respective access control. For more information on access controls, see *Embedded Web Server Administrator's Guide* for your particular device, at https://support.lexmark.com.

Examples of functions whose access can be controlled are the following:

- Copy
- E-mail
- Scan to Fax
- Fax
- FTP
- Held jobs (such as confidential print jobs)
- Flash drive printing
- Flash drive scanning
- Initiating scans remotely

Device management functions can also be restricted with access controls. Examples of device capabilities that can be controlled are the following:

- Remote management
- Firmware updates
- Applications configuration
- Embedded Web Server access
- Importing or exporting all settings
- Out of Service Erase

Applications can also be restricted with access controls. Examples of app settings that can be controlled are the following:

- New Apps
- Scan Center

Active Directory

Overview

Microsoft Active Directory support is provided on solution-enabled Lexmark devices (models with touch-screen displays). Using Active Directory for the latest generation of Lexmark touch-screen devices is a secure method of authentication and authorization. It is also simpler to set up and easier to manage for administrators. Active Directory authentication is provided by Lexmark's support for Kerberos at the firmware level.

Benefits

- Simplifies network setup and PKI enrollment
- Automatically creates and configures LDAP+GSSAPI and Kerberos authentication
- Enhances fault tolerance with automatic detection of multiple domain controllers
- Let's you get certificate chains from the domain controller by automatic download
- Supports Single Sign-On with authentication credentials, simplifying user access management

Details

With Active Directory, the joining process is greatly simplified. Setup is performed from the device EWS and requires a few basic settings (domain name, administrator username and password). The required LDAP

+GSSAPI and Kerberos setup is completed automatically using data from the Active Directory domain controller. The device is joined to Active Directory by establishing computer credentials. This setup creates a secure connection while reducing the burden on IT administrators, who no longer need to issue or manage service accounts for each device.

More key distribution centers (KDCs) in the environment are included in the Kerberos configuration file of the device and are used if necessary. This arrangement also permits devices to use the optimal selection from the domain controllers detected in the environment. The device automatically downloads domain controller CA certificate chains. The device maintains it (if certificate monitoring is specified) by periodically verifying that the certificate chain is up to date.

Active Directory participation permits the usage of Single Sign-On. If already logged into the Active Directory environment, the EWS can use directory integration to authenticate the user automatically and securely. This authentication support is extended to other token types, such as using card readers for access to the EWS.

For Lexmark's current firmware generation, the process is further simplified, allowing you to select automatic setup of more security services from the Active Directory joining screen.

- If the LDAP address book is selected, then the LDAP server address book information is configured with Active Directory server data.
- Active Directory users and groups are automatically available when configuring authentication and authorization on a device that has been joined to a domain.
- After joining a device to an Active Directory domain, enable CA Certificate Monitoring to obtain the certificates from the domain controller and monitor for certificate updates.

Secure LDAP

Overview

When scanning to e-mail or scanning to fax, you can select the recipient's e-mail address or fax number rather than manually typing it. This important convenience is made possible through LDAP. With LDAP, an MFP can query the corporate directory for information. The use of TLS protocol adds security to the process. By establishing an TLS connection before generating LDAP queries, an MFP and the directory server can protect the information they exchange.

Benefits

The benefits of using LDAP over TLS include:

- The information queried by an MFP is secured (encrypted) on the network.
- MFPs can leverage your existing PKI infrastructure to perform TLS, conforming to your standard security practices.

Details

All LDAP traffic to and from Lexmark devices can be secured with TLS to preserve its confidentiality and privacy. LDAP information that is exchanged over a TLS connection, such as credentials, names, and e-mail addresses and fax numbers, is encrypted.

MFPs can be configured to trust a 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. MFP configurations dictate that the MFP precedes all LDAP traffic with the negotiation of an TLS connection. The directory server provides its certificate, the MFP validates it and a secure encrypted communication channel is established. All subsequent LDAP traffic moves over this channel, so all LDAP information is encrypted on its network. This applies to LDAP queries for e-mail and fax information, as well as LDAP-based user authentication.

Automatic insertion of sender's email address

Overview

When a user selects a function on an MFP, such as Scan to Email, the MFP can require authentication (login) before proceeding. While the device performs authentication, it also queries the user's information and automatically populates an email address in the From field of the scan job. By automatically populating the From field of the outgoing email, the user is identified as the email recipient.

Benefits

Anonymous emails are eliminated by inserting the identity of the authenticated user in the email generated with the Scan to Email function.

Details

Automatic insertion of email addresses in the From field of outgoing emails provides a form of nonrepudiation by automatically querying the authenticated user's information. Lexmark devices can use various protocols to validate and look up user information: LDAP, LDAP over TLS, LDAP+GSSAPI, or Active Directory. Using any of these authentication protocols enables devices not only to authenticate but also to query that same user information in the directory server. If the device locates the user's email address, then it populates the From field with the user's email address. The user can then use the Scan to Email function. If the device cannot locate the user's email address, then the device does not allow the user to proceed with the function.

Login attempt limiting

Overview

You can limit the number of failed login attempts to Lexmark devices to prevent unauthorized access. This capability can help reduce the risk associated with password attacks on user accounts. In addition, the device can be configured to require a set time before allowing users to retry access attempts. These tools are especially useful if the customer environment does not have an identity management service capable of locking down user accounts after multiple failed attempts.

Benefits

- Mitigates risks associated with brute-force attacks on user passwords by limiting the number of login attempts
- Specifies a minimum time before any additional password entries can be accepted

Details

You can inhibit password attacks by limiting the number of failed login attempts within a specific time frame. Imposing a lockout time before more logins are permitted further inhibits attacks. Also, after a valid user is logged in to the device, inactivity timers are enforced to ensure that users are logged out in a timely manner. The device can be set up to track user accounts being attacked and the time and frequency of the attack, and the devices where the attacks occurred.

Control panel lock

Overview

You can place a Lexmark device in a locked state so that the control panel cannot be used for any user operations or configuration. Users cannot copy or scan. If the device has a hard disk, then incoming print and fax jobs are stored in the hard disk instead of being printed. This setup prevents incoming jobs from being exposed in the output bin. Users can unlock the device by entering their user credentials to release held jobs.

Benefits

- Devices can be secured with a simple method so that during off hours, scanning and printing operations are not allowed.
- Jobs printed to a locked device cannot be stolen from the output bin.

Details

The control panel lock enables or disables the associated FAC (permission) that is accessed through the device EWS. The FAC lets administrators limit access by requiring a PIN, a device password, or network credentials to lock or unlock the device at its control panel. This feature requires the installation of a hard disk.

When a device is locked, the control 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 in the device hard disk. If hard disk encryption is enabled, then the jobs stored in the hard disk are encrypted. When the device is unlocked, jobs received during the locking period are printed. Any confidential print jobs received during the locked period are not printed. They are available through the Confidential Print Job interface on the device control panel.

Confidential Print

Overview

The Confidential Print feature addresses the basic concern of printed pages left on the device for anyone to pick up. With Confidential Print, the device securely holds submitted jobs until the intended recipient is present at the device and enters the proper PIN code on the device's control panel.

Benefits

- Ensures that jobs are only printed when the authorized recipient is at the device.
- Operates whether the device is equipped with a hard disk.

Details

Lexmark device drivers can be directed to submit confidential print jobs by specifying a confidential four-digit print PIN. This is a standard feature on Lexmark devices and drivers. When a device receives a confidential print job, the data stream is stored in the device's random-access memory (RAM) or in the device hard disk. Jobs stored in the device RAM are deleted if the device is turned off and can be deleted automatically by the

device if a memory shortage is encountered. For these reasons, it is strongly recommended that a hard disk be installed if the Confidential Print function is to be used extensively.

When a storage device is present, jobs are retained across power cycles, greatly increasing the number of jobs that can be held. Jobs buffered to a storage device uses the security of encryption, including maintaining confidentiality of buffered jobs even after moving the storage device to another print device.

For more security, setting a maximum number of retries on a PIN prevents brute-force attempts to guess the PIN. If a PIN is entered incorrectly after the specified number of times, the corresponding print jobs are deleted. Also, with the Job Expiration feature,

your jobs can be automatically deleted from the device after a specified time interval, ranging from one hour to one week.

Secure Internet Printing Protocol

Overview

Secure Internet Printing Protocol (IPPS) protects Internet Printing Protocol (IPP)–based print jobs and printer queries by providing TLS data encryption and user authentication.

Benefits

- Encryption for all IPPS traffic
- Forced user authentication to use IPPS

Details

IPP is a standard protocol, operating over TCP port 631, that lets clients query printer capabilities, submit print jobs, and query device and job status. To secure this potentially confidential data, the IPPS protocol is available. Enable this protocol by setting the Internet Printing Protocol FAC permission.

After IPPS is enabled, clients are upgraded from unencrypted connection to TLS on port 631 and are required to authenticate before any further communication is permitted. Communications are encrypted before authentication to protect credentials, and all IPP traffic is TLS encrypted.

Incoming Fax Holding

Overview

With the Incoming Fax Holding feature, MFPs can receive faxes and hold them until they are released. Devices with a hard disk can be configured through a scheduling menu to store received faxes temporarily rather than immediately print them. These held faxes are secured until the designated release time has elapsed or proper credentials have been entered on the Lexmark device. This feature ensures that the fax output is not exposed to unauthorized persons during off hours.

Benefits

- Determines when faxes are automatically printed or held for authorized release
- Secures fax output to prevent use by malicious individuals

Details

The Incoming Fax Holding feature is enabled in the Holding Faxes menu. This menu also lets the device administrator schedule when to hold faxes and when to print them.

To schedule fax holding, do the following:

1. From the home screen, touch Print Faxes or Hold Faxes.
2. Select the day and time. For example, after work hours and weekends.

For added security, the administrator can require a user or a group to authenticate before releasing the faxes. This configuration lets the administrator ensure that the faxes are released to authorized individuals and audit the action if there are concerns about malicious use.

Secure start process and operating system protections

Overview

Security is a part of the Lexmark development process and is therefore a standard offering on all Lexmark devices. Lexmark is committed to developing security mechanisms around device operating systems, firmware updates, and embedded solutions. Device security is not an afterthought and must be holistic, which includes protection against malware and viruses. Lexmark devices accomplish this level of security by verifying the firmware and processes in memory and taking corrective action if any threat or tampering is detected. These checks occur during startup and during normal operation of the device.

Benefits

- Ensures that there is virtually no option for loading malware or viruses in the operating system or other operating firmware of a device
- Ensures that only trusted firmware is installed on Lexmark devices by using digital signatures and other security mechanisms
- Stops operation and reports an error if self-checking detects its security is compromised

Details

Lexmark devices operate on a Linux-based platform. Lexmark modifies the kernel and underlying services so that the operating system can better meet the needs of its devices, including adding security features. This approach provides hardening against external attacks.

Also, Lexmark uses the AndroidTM open-source project to drive the graphical user interface of the control panel of the current generation of touch-screen devices.

Other protections used in the development of the Lexmark operating system platform are the following:

- Some server applications that are found in standard Linux distributions have well-documented security exposures and are subject to rootkit attacks. When possible, these applications are removed by Lexmark's firmware security team to reduce the potential attack surface on devices.
- Lexmark development teams create custom applications that control functions such as print, fax, copy, and scan. After all modifications are made to the operating system, it is firewalled and hardened to the point that the embedded environment is closed.
- If a vulnerability is found on a device or more functionalities are added to the operating system, then a firmware update replaces the entire operating system.

Only trusted firmware can be loaded on a Lexmark device. The following requirements are defined so that significant protections are provided with the device firmware:

- The data must be packed appropriately in a format that is specific to the device type.
- The firmware is encrypted and signed with private keys that do not reside on the device. A corresponding public key, which does reside in the device firmware, is

used to decrypt the firmware and verify its signature. The digital signature provides two protections: validating the firmware came from Lexmark and ensuring that the firmware has not been modified since it was created. To install a malicious firmware image, an individual must have this private key, which is not published outside of Lexmark.

- On each boot, each stage in the boot chain verifies the signature of the next stage, beginning with a hardware-anchored root of trust and a public key therein. These digital signatures provide run-time firmware integrity, in addition to the install-time integrity described above.
- Firmware updates can be restricted to authenticated and authorized users or disabled through the device FAC.

Lexmark developed the following chain-of-trust process to validate the integrity of a device operating system during startup, normal operation, and execution of an internal application. If any of the following tests fail, then the device halts operation of all processes and reports an error.

- The physical hardware is used to validate the secure bootloader, which is then used to verify the signature on the kernel.
- The kernel is then used to verify the signatures on each firmware flash partition before it is mounted by the device.
- Internal device drivers and executable code are operated on trusted read-only flash partitions. No code is ever written to a standard or optional device hard disk.
- Each time a block is paged from the trusted flash memory to RAM, its hash value gets verified by the kernel. This action provides continuous verification and tamper detection.

The following are other protections that Lexmark has in place to protect the device operating system:

- If the device is compromised, then the usage data is placed in tamper-proof memory so that it can be analyzed.
- All devices use non-x86 processors, limiting execution of commonly available exploit binaries.
- The device does not accept incoming email, nor does it contain its own SMTP server or service. Likewise, Lexmark devices can only perform SMB client operations and do not act as SMB servers.
- The device hard disks (standard or optional) are not designed to be long-term storage devices. They also do not allow users or administrators to load or extract information, or to create or share folders or FTP information to the hard disk.
- Disk encryption is enabled by default when a Lexmark device ships with a hard disk.
- The device does not allow incoming remote procedure calls (RPC), which limits the propagation of malware from other devices. The device does not recognize or run files with executable extensions. Image files, such as BMP, DCX, GIF, JPEG, JPG, PCX, PDF, PNG, TIF, and TIFF are recognized as print-related data.

eSF application security

Overview

You can extend the capabilities of Lexmark devices using the Lexmark Embedded Solutions Framework (eSF). Included in Lexmark solution-enabled devices, this execution platform allows function enhancements to devices through the loading and running of custom applications. These applications are loaded and configured on the device. To ensure that device security is not compromised, well-defined interfaces and an application certification process are specified, and only encrypted, signed application packages are created.

Benefits

- Device functions are enhanced by installing eSF applications in a secure manner using signed, encrypted files that are verified by the device before installation.
- Device function usage by eSF applications is restricted to well-defined APIs.

Details

Lexmark devices inspect all downloaded firmware packages for required attributes before adopting or executing them. eSF applications are delivered to devices in the same way. The application must be packaged appropriately in Lexmark's proprietary format. Also, packages are encrypted with a symmetric encryption key that is known only to Lexmark and is embedded securely in all devices. All application packages must include multiple digital 2048-bit RSA signatures from Lexmark. If these signatures are not valid, then the application is rejected.

Lexmark eSF applications can be transmitted over the network, which allows all devices on that network to be updated efficiently. This process can be automated and scheduled, and does not require someone to be at each device. The device receives the application, validates it, adopts it, and stores it automatically.

For security, you can restrict the ability to install, update, or remove applications. First, eSF flash files are subject to the same firmware update access control as other firmware update flash files. So if this access is disabled, then eSF applications cannot be installed except through the EWS. Then you can use access controls to limit access to the EWS to authorized administrators only.

The security of the application also relies on a secure development and certification process. This process ensures that the application performs the intended function, and prevents malicious malware, viruses, or undesired behavior. Most eSF applications are developed by Lexmark, but even applications developed by third parties are verified for acceptable behavior and adherence to device and memory restrictions. Only after approval is the application packaged and signed by Lexmark for distribution.

Protected USB ports

Overview

USB ports on personal computers provide a means to connect devices of various types for various interactions. However, for security reasons, the USB ports on Lexmark devices are far more limited in their capabilities.

The USB host ports on Lexmark devices do the following:

- Detect an inserted USB mass storage device (flash drive) and show the image files or flash files that are stored in the device.
- Select a supported image file for printing or select a valid flash file to initiate a firmware update (if permitted by security settings).
- Scan data directly to the flash drive.
- Permit or restrict access based on a defined schedule. If enhanced security is required, then the device can limit or deny these operations, or deny any use of USB devices.

The USB host ports on Lexmark devices do not permit the following operations:

- Connecting and using any form of USB device except a mass storage device, card reader, or human interface device (HID), such as a keyboard
- Submitting or processing of PCL® emulation, PostScript emulation, or other printer data stream files
- Submitting of any other sort of data (executable code, configuration files, and so on)
- Recording any sort of data from the printer to a USB-attached device other than direct scanning to a flash drive
- Executing a code from a USB-attached device
- Booting the printer from a USB-attached device
- Transferring data between a USB-attached device and the network to which the printer is attached (except where the USB port is configured for smart card authentication)

Disabling the front USB port is an option at manufacturing or by the device administrator during setup using access control restrictions. Some Lexmark devices also have a rear USB host port. The use of this port is restricted to card readers and HIDs, such as a keyboard.

Benefits

- Carefully controlling environments where sensitive documents exist by not permitting users to perform scan-to-USB operations
- Restricting users from performing print-from-USB operations in environments where printing is tracked or allowed only on a paid basis
- Limiting the ability to perform scan-to or print-from USB devices to authenticated users only
- Preventing the use of any USB memory device in highly restricted environments

- Eliminating virus and malware attack vectors
- Scheduling when the USB ports are available for usage

Details

In general, USB support on Lexmark devices is unlike USB support on personal computers. Personal computers typically support a wide array of devices through USB ports, such as keyboards, mice, monitors, hard drives, speakers, network cards, and digital cameras. The flexibility offered by USB host support on personal computers is not needed—or desirable—on printers.

The USB host port on Lexmark devices is intended to allow convenient printing and scanning of image files. It also allows attachment of card readers and HID, such as keyboards, for authentication and authorization, and enables fast, easy maintenance activities for technicians.

The supported image file formats are BMP, DCX, GIF, JPG, PCX, PDF, PNG, TIF, and TIFF. The device firmware and the USB host port implementation are carefully designed to restrict the use of the port for any other purpose. Several factors in the device design provide for that protection, including the following:

USB support is limited

When a USB device is connected to the USB host port of a Lexmark laser printer or MFP, a process known as enumeration occurs. The device indicates its USB device class to the host so the host knows how to communicate with it.

Lexmark devices support only USB devices that belong to a mass storage device class and HIDs for simple input, such as keyboards and authentication card readers. Lexmark devices also support specific chip card interface device (CCID) card readers used for authentication. So, if a device such as a USB network card is

inserted, then the printer does not establish a connection to it. An exception to the network adapter restriction is Lexmark's available wireless adapter, used to provide Wi-Fi network access to a printer. This device is uniquely recognized by the enumeration process and is allowed to connect and function normally.

Flash drives are a typical example of the sort of device that you might expect to use with Lexmark devices. These devices are widespread today and are generally supported by printers and MFPs.

USB storage devices that are SCSI-compliant use the FAT32 file system and do not include an embedded hub. So they are likely to be recognized and compatible with Lexmark devices. If a USB device does not meet these requirements, then the printer or MFP rejects the external drive.

Support is limited to printing image files, direct flash drive scanning, and updating firmware through flash files

When a flash drive is inserted into a device USB port, the device examines the drive's file system and lists any image and firmware files. No other type of file is supported. Files that contain PostScript emulation or PCL emulation data streams are not supported. When a user prints a file, the contents of the file are read from the USB-attached device and transferred to the appropriate image interpreter. This component of the device firmware inspects the format of the file and discards files that are not of the expected format. Firmware files are accepted on the device only if signed by

Lexmark, ensuring that tampered firmware can never be installed on a device. This process eliminates any opportunity to submit a file by mislabeling it. In other words, it is not possible to load executable code in the printer by storing it in a file called, for example, HarmlessJob.pdf.

Image files are handled internally, as if they were submitted to the device through any of the other device ports (parallel, network, and so on). Therefore, the USB host port does not provide any avenues for submitting data that does not exist.

The USB host port is less forgiving because the printer decides whether to show and allow the submission of data through the USB connection. Unlike other connections, the printer determines what can be sent to it through the USB port.

There is no support for submitting executable code, code updates, configuration changes or anything other than the supported image files to the printer through the USB port.

No support for startup from USB-attached devices

On many personal computer systems, the USB host port is included in the list of partitions that can be used for startup. That is, you can potentially start such computers from a flash drive. However, this capability is not permitted with Lexmark devices. The USB ports are not included in the startup sequence.

No support for network interaction with USB-attached devices

A USB-attached device cannot exchange data in any way with the network to which the device is attached. There is no facility for passing data from the USB-attached device to the network or from the network to the USB-attached device.

The only exception is for cases where the printer or MFP provides authentication capabilities through an HID, such as a card reader for card-based authentication. In this instance, an embedded application is installed through the Lexmark eSF on the printer or MFP. This application lets the device interface solely with a directory server to validate a user's identity. Then the device pulls information associated with the authenticated user, such as email address and home directory information, and identifies privileges.

Limited text character input from standard USB keyboards is permitted with the HID interface. But this input is used only as a substitute for the on-screen keyboard supported in devices with touch screens.

No support for adding more drivers or functionality

The functions in USB-attached devices that are permitted are controlled by the device firmware, which is not customizable or extensible by the end user. The firmware does not permit the addition of arbitrary executable code of any sort.

Firmware updates are supported through the USB port on the back of the device through the network interface. These updates must include multiple digital signatures to ensure that the device accepts only code that is produced and provided by Lexmark. There is no support for adding additional USB drivers to the device to alter its function.

The USB host port can be disabled

In some environments, controlling the submission of print jobs (including image files) is important, and all uncontrolled avenues by which jobs can be submitted are undesirable. For example, a college library might allow users to submit print jobs

over the network and then charge them for the pages they print. In such a case, it is unacceptable to let users walk up and submit jobs to the printer from a flash drive.

Administrators have two options for disabling the function of the USB host port entirely. The first is for Lexmark to disable the port during the manufacturing process. In this case, the port is permanently disabled and cannot be reactivated by the device administrator or end user under any circumstances.

The second is for the device administrator to disable the security permissions menu on the device EWS. In this case, the port can be enabled again later, if necessary. The function of disabling or enabling the port can be restricted so that end users cannot reenable the port.

Lexmark devices support the use of portable flash drives for scan-to-USB or print-from-USB tasks. Device configurations cannot be changed or exported with USB devices. The ability to scan to or print from USB devices can be controlled separately by managing permissions through the Security menu.

Secure Data

Overview

To meet today's complex printing requirements, Lexmark devices are equipped with nonvolatile memory to store essential system information when the devices are turned off. Lexmark devices can be equipped with various internal storage options, such as intelligent storage drives and hard disks. Internal storage options also let you run some printing applications or printer software solutions. The use of internal nonvolatile memory and storage is an industry-standard method for enhancing the performance of print and imaging devices.

Internal storage options on Lexmark devices are designed for device-specific functionality and cannot be used as long-term storage for items unrelated to printing and scanning. The device architecture does not allow extracting information, creating folders or file shares, or serving FTP data from a Lexmark device.

Internal storage is primarily designed to store print or image data, font data, forms data, macros, and sometimes job data. In addition, Lexmark uses internal storage to buffer data in scan, fax, and copy jobs. In general, print-related data is processed in RAM, except when the job exceeds the amount of RAM on the device. The other exception is if you enabled the Confidential Print or Print and Hold feature through the print driver.

Lexmark has defined mechanisms and processes to enable the following:

- Protection of data stored in on-device permanent memory
- Removal of that data securely and permanently when it is no longer required
- Hindering malicious users from gaining physical access to the storage device

Understanding user data encryption

Starting with FW23, when enabled, User Data Encryption (UDE) encrypts internal storage and service nonvolatile memory. The internal storage and nonvolatile memory are used to store user data, settings, and licenses. UDE allows Lexmark devices to comply with the new Common Criteria protection profile requirements for hard-copy devices.

Encrypted internal storage options

By default, internal storage options installed on Lexmark print devices are encrypted. The device internally generates a 256-bit Advanced Encryption Standard (AES) key, used to encrypt all data. The key is stored noncontiguous on the device, or beginning with FW23, in the Trusted Platform Module (TPM). This key makes the contents accessible only on the original device. The data on a stolen component would not be accessible even if it was installed in an identical device model.

Benefits

- Increased security of active and residual data.
- There is no delay for cleanup or post-processing after jobs are finished because hardware-assisted encryption is applied.
- The encrypted data is device specific and is not transportable.

Details

Encryption protects against the threat of removing the internal storage option from the SFP or MFP, and attempting to gain access to the data it contains from another device.

The encryption key to be used, 256 bit (AES symmetric encryption), is pseudo-randomly generated. The key is stored securely either on the device or, beginning with FW23, in the device TPM. The internal storage option is then reformatted with the encryption key. Any data on the internal storage option is lost. The encryption key is generated on the device and stored separately from the storage component itself. The decryption fails if the internal storage option is removed and placed in another Lexmark device. The failure happens when the internal storage attempts to validate and use the secondary Lexmark device key.

After failing to decrypt the storage option, the Lexmark device prompts the user to reformat it with a new encryption key. This action destroys the existing encrypted data on the storage option.

Understanding the intelligent storage drive

Beginning in 2022, Lexmark introduced new products that included support for the intelligent storage drive (ISD), a solid-state flash storage option for Lexmark printers. ISD provides solutions previously offered through add-on card modules. The ISD offers several security features:

- The ISD is encrypted by default. The printer internally generates a 256-bit AES key. It also encrypts all user data on the ISD. The key is stored in the TPM on the printer, making the contents of the ISD accessible only on the original printer.
- The data on a stolen ISD is not accessible even if the ISD or TPM is installed in an identical model of the printer.
- Due to the nature of flash memory, automatic disk wiping is not supported on the ISD.
- Installation of a traditional hard drive erases and disables the user data portion of the ISD. However, users can continue to use the solutions functionality. These solutions include storage of highly specialized fonts.

- The ISD storage uses a secure cryptographic erase of user-related data. When initiated, the ISD encryption key is destroyed, preventing access to any sensitive data.
- For even greater security, the ISD can be combined with the TPM to protect against insider threats and malicious attacks. The TPM provides enhanced encryption capabilities to the ISD. TPM securely stores ISD encryption keys on separate hardware from the data that they protect.

Benefits

- An installed ISD supports most solutions delivered for free.
- ISD delivers powerful functionality that simplifies solution installation without extra required hardware.
- Enhances free access to features that are available with ISD installation that previously required purchasing a solutions card.
- Delivers greater capabilities with modern storage technology that is faster and more energy-efficient.
- Simplifies installation with a new and more efficient way to install multiple card solutions.
- Allows digital licensing for features such as IPDS and Bar Code.
- Supports double-byte character set (DBCS) font and CVS fonts for the following languages:
  - Arabic
  - Chinese
  - Hebrew
  - Japanese
  - Korean
- Includes Forms, Forms Merge, and PRESCRIBE support, and magnetic ink character recognition (MICR) as a standard feature.

Understanding intelligent storage drive wiping

An intelligent storage drive (ISD) wipe is a cryptographic erase of the user data partition. During this operation, the ISD encryption key is destroyed, preventing access to any sensitive user-related data, which includes user flash and job data. Lexmark uses this method of wiping to minimize wear on the drive itself.

Overview

The cryptographic erase function destroys the encryption key that is used to encrypt the user data partition of the ISD. Because the key is destroyed, it prevents the ability to gain access to any information contained on the user data partition.

Benefits

- Minimizes risk of information exposure when the device is retired, recycled, or otherwise removed from a secure environment.
- Extends the life of the device itself.

Details

The Erase Intelligent Storage Drive function initiates the destruction of the cryptographic key that protects data stored on the user data partition of the ISD. This function is available only in devices announced in 2022 or later. In later firmware versions, the Out of Service wiping function is available on the Embedded Web Server. Out of Service Erase is often configured as an administrator-only operation through a function access control.

When the key for the user data partition is destroyed, a new key is generated. The ISD user data partition is encrypted using the new key. After the operation is completed, it prevents the ability to access any information previously stored on the ISD user data partition.

The cryptographic erase function does not erase, sanitize, or overwrite the enhanced partition of the ISD that contains highly specialized fonts.

Printer hard disk

For most devices, Lexmark offers a hard disk option that is used to buffer print jobs, collate large jobs, or to store forms, fonts, or macros.

This storage option is ideal for organizations that prefer to use traditional hard drive technologies to sanitize residual data. Traditional hard disks are used for various purposes, including buffering scanned data during copy jobs and buffering print data during print jobs. Protecting buffered data ensures that no one can access potentially sensitive information contained in image scans or print jobs that the device receives.

As mentioned in the section on encrypted storage, Lexmark devices can encrypt all data on hard disks to protect it from external access. This action protects not only the residual data that remains after printing jobs but also the data that is actively being used. This feature prohibits someone from turning off the device in the middle of a job and using the data that is left on the hard disk.

When a traditional hard disk is installed, the storage portion of the ISD is disabled. However, users can continue to leverage the card functionality, which is used to store solutions and licenses.

Hard disk file wiping

File-based disk wiping sanitizes the portion of the hard disk where job data is stored after processing so that no residual data can be read.

In contrast, the following erasure options erase the entire disk:

- Complete—For more information, see **"Complete hard disk erasure" on page 45**.
- Out of Service—For more information, see **"Out of Service wiping " on page 47**.
- Sanitize all information on hard disk—For more information, see **"Nonvolatile memory wipe" on page 45**.

Lexmark devices offer single-pass or multiple-pass wiping that is compliant with the National Institute of Standards and Technology and U.S. Department of Defense guidelines.

26WWM13805

Overview

Lexmark devices containing a traditional hard disk support the hard disk file-wiping functionality. Lexmark uses hard disks on devices to temporarily buffer scan, fax, print, and copy data that exceeds the amount of RAM installed on the device. Buffered data can be deleted from the hard disk immediately after completing an original

scan, fax, print, or copy job, or at other times as specified.

If you use Confidential Print and Hold features when fax jobs are received and sent, the devices can temporarily hold print jobs on a hard disk. This data remains on the hard disk until you print or delete the job, or until the document expires through the job expiration feature.

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, theoretically, can be recovered with substantial effort. Lexmark devices support an additional mechanism for protecting residual data—hard disk file wiping. Hard disk file wiping actively overwrites any job data files that are deleted. You have a choice of single or multiple passes of data, which remove all data residue from the deleted file.

Some Lexmark devices let you select when hard disk file wiping is activated (automatic, scheduled, manual). Others automatically delete a file permanently, immediately after it is no longer required for the job. Disk wiping erases only job data from a device hard disk that is not currently in use by the file system. All permanent data on the device hard disk is preserved, such as downloaded fonts, macros, and held jobs. The Lexmark wiping process adheres to NIST and DOD (DOD 5220.22-M) guidelines for overwriting confidential data.

Benefits

Increased security of residual data.

Details

- **Automatic**—Immediately overwrites areas of the disk that were used for job processing. Automatic wiping marks all disk space used by a previous job and prevents the file system from reuse this marked space until it is sanitized. Automatic wiping is the only wiping process that operates without having to take the device offline during the wiping process.
  Single-pass and multiple-pass settings determine the number of overwrite passes that are used during the wiping process. Highly confidential information must be wiped only with the multiple-pass method. Multiple-pass wiping takes longer than the single-pass version because more overwrite passes are used.
- **Scheduled**—Lets administrators select when to execute the disk wiping of previous job files. When the disk space that is used for a job is no longer required, it is marked for wiping later. At the first available non-busy period after the next scheduled-time setting, the device goes offline and begins the disk wiping process for any marked disk space. No user warning or confirmation message appears. Both the Manual and Scheduled settings enable the file system to reuse marked disk space without wiping it.

- **Configurable Single- or Multiple-Pass Disk Wiping**—Automatic hard disk file wiping can use either a one-pass, three-pass, or seven-pass wipe. Single-pass wiping only replaces the data with zeros, whereas multiple-pass wiping includes more methods of sanitization. Multiple-pass wiping meets the NIST/DOD/DOE standards for confidential data (DOD 5220.22-M, Section 8-306).

Complete hard disk erasure

Overview

"Complete" or "Sanitize all information on hard disk" erasure wipes clean the entire hard disk. Lexmark recommends performing a complete hard disk erasure process before a device is taken out of service or removed from any current location. This function is different than the methods previously described. With the "Sanitize all information on nonvolatile memory (or hard disk)" (also called "Complete Wipe Disk" or "Erase Hard Disk") command, you can eliminate all contents of a disk.

Benefits

- Minimizes risk to exposure of information when the device is retired, recycled, or otherwise removed from a secure environment
- Completely removes all residual customer data from the hard disk
- Details

Lexmark recommends erasing the memory installed in your Lexmark device when the device is:

- Decommissioned
- Having its hard disk replaced
- Being moved to a different department or location
- Being serviced by someone outside your organization
- Being removed from your premises for service

Nonvolatile memory wipe

A nonvolatile memory wipe erases the memory of a printer. Lexmark devices use two forms of nonvolatile memory—electrically erasable programmable read-only memory (EEPROM) and "Not AND" (NAND). These components store the device operating system, device settings, network information, embedded solution applications, various scanner settings, and bookmark settings.

Note: No user-related print copy, or scan data is stored in nonvolatile memory.

Overview

The printer-memory-erasing function deletes all content stored in the various forms of flash memory on your device. (The function is called "Erase Printer Memory," "Wipe All Settings," or "Erase all apps and app settings,"

depending on the device model.) You can completely clear all settings, solutions, and job data on the device. This function is ideal when retiring, recycling, or removing a device from a secure environment.

Benefits

- Device settings are restored to the factory default settings, removing any setting values that may be incorrect.
- Printer-memory erasing enables a complete reset, which permits movement and reinstallation at another location with no residual settings retained.

Details

The "Erase Printer Memory" ("Wipe All Settings") function is a tool for erasing all contents stored in the various forms of nonvolatile memory on a device. "Wipe All Settings" is accessed on the device control panel in the Configuration menu. "Erase Printer Memory" is accessed through the Embedded Web Server in the Restore Factory Defaults menu or the Maintenance menu (for new devices). It is also included in the Out of Service Wiping (Out of Service Erase) function. Using "Erase Printer Memory" ("Wipe All Settings") completely clears all device settings, including network and security settings. Installed applications and their settings are removed. Applications shipped with a device remain, but their settings are reset.

The latest line of Lexmark devices allows more granularity for clearing the nonvolatile memory of a device.

Trusted Platform Module

Overview

Lexmark security features help keep information safe—in the document, on the device, over the network, and at all points in between. Beginning with the new product announcements for 2022, devices now include a standard Trusted Platform Module (TPM). The TPM delivers authentication, system integrity checks, and cryptographic capabilities to create a unique digital system fingerprint.

The TPM is quickly becoming the industry standard for enterprise hardware security. It provides a more secure experience for users by storing hard disk encryption keys on a piece of hardware other than where the data is stored. This arrangement adds more layers of protection. This hardware also helps make encryption stronger with enhanced random number generation. Lexmark Cloud Services and other applications also use it to securely identify devices in the future.

The TPM, now standard, was an option for various Lexmark models that were announced in 2018 and later.

Benefits

The TPM strengthens the ability of Lexmark devices to secure information, whether stored in the device or being transmitted to or from the device. The TPM provides improved capabilities in generating and securing the cryptographic keys that are used by the device.

TPM immediately satisfies many corporations or government agencies that need to have certification of device cryptography.

- Random number generation is stronger.
- The key store for certificates and encryption keys is secure.
- The hard disk encryption key is protected by the TPM.

- TPM will be a requirement for future Common Criteria and FIPS PUB 140-2 validations.

Out of Service wiping

The Out of Service command lets you wipe device memory in one step when removing the device for service or from a secure environment.

The options are:

- **Erase Printer Memory**
- **Erase Intelligent Storage Drive**—Available in devices announced in 2022 and later with an installed ISD.
- **Erase Hard Disk**—Available if a hard disk is installed in the device.

To ensure no customer data remains on the device, use both the Erase Printer Memory and the Erase Intelligent Storage Drive or Erase Hard Disk options. You can choose to initiate both functions at the same time from either the Configuration menu or the Embedded Web Server.

Benefits

It provides a simplified process to prepare the device for removal from service or a secure environment.

Details

This operation is available if the appropriate function access control has been set for the logged-in user. Out of Service Erase options can be found in the Maintenance menu under Device settings on both the Configuration menu and the EWS. Before initiating the wipe process, the device provides a predicted total time

for the disk wiping to complete. The time remaining before completion is also shown while the wiping is in progress.

Physical lock support

Lexmark devices support cabled computer locks, which you can use to secure critical and sensitive components physically. These components include the controller board and hard disk.

Benefits

- Protects against malicious access to the critical device components, such as the hard disk, controller board, optional memory (flash or RAM), fax modem, and network card
- Reduces the threat of a hard disk being stolen from a device

Software and Solutions

Lexmark has developed a rich supporting ecosystem of software and solutions designed to complement its extensive device security capabilities. This support includes on-device software to provide advanced features such as smart card authentication, print job encryption, and print release for users.

Lexmark's device management tools enhance the security of the device and the customer environment through the following features:

- Automated certificate management
- Device discovery and settings enforcement
- Fleet-wide firmware updates

Print Release application

Overview

With Lexmark Print Management, employees send print jobs from anywhere—including their desktops, tablets, or smartphones. LPM also lets you release the jobs for printing whenever and wherever they are ready. This feature means that confidential information stays protected, as potentially sensitive print jobs do not pile up unnecessarily on office printers.

With Print Release, all documents are held in a print queue until their owners release them. Depending on your organizational policies and security risk profile, the queue can be hosted on premise or in the cloud, which offers more features and benefits. Documents can be released from any enrolled device, from anywhere. To release held documents, users are required to either swipe an ID badge or type their credentials at the device. Then they select a job from the queue for printing.

Benefits

- Determines when documents are automatically printed or held for authorized release
- Deletes unprinted documents from the print server after a set time to prevent held or draft documents from being seen by unauthorized persons
- Integrates with enterprise identity systems for secure authentication
- Restricts printing of draft documents with confidential information
- Increases flexibility for employees
- Strengthens access controls to improve security and compliance
- Scales easily with on-premise, secure cloud, or hybrid deployment

Details

This solution consists of an externally hosted document management application (either on-premises or at Lexmark's cloud services) and a device-resident application. This solution provides the local user interface to permit selection and release of the wanted print jobs.

26WWM13805

PrintCryption

The Lexmark PrintCryption solution heightens security in sensitive environments through end-to-end encrypting of print jobs at the workstation, in transit, and on the device. This level of printing security is ideal

for businesses handling highly confidential, personnel, financial, medical, technical, and proprietary business information. PrintCryption also enables better compliance and supports multiple levels of AES encryption for a balance of performance and confidentiality. The solution is available to customers for no cost.

The solution also works for direct printing. During the initial driver install and configuration, the print driver retrieves the public key of the printer. When a user prints with "Job Encryption" enabled, the print job is encrypted using 128-bit or 256-bit AES encryption. The print job is also protected from tampering by using HMAC-SHA256. To add one more layer of protection, the AES and HMAC keys are encrypted with the public key of the printer. Then the job is sent to the printer, where the print jobs are checked for integrity, decrypted, and then printed.

PrintCryption 2.0 supports the following:

- Two levels of encryption: standard (128-bit AES) and enhanced (256-bit AES)
- HMAC-SHA256 job digests appended to payload to verify that the payload has not been modified (prevent tampering)
- RSA-2048 public key encryption (encrypts AES and HMAC (Hashing for Message Authentication Code) keys)

Solution	Reference
Lexmark UPD (Universal Print Driver) v3.0.0.0 and later	Specifically for the Microsoft Windows operating system only. For more information, see Lexmark UPD.
PrintCryption 2.0 eSF application (82S1217)	See **Lexmark Cloud Package Builder Site.**
PrintCryption - Native in firmware	FW8.1 or above.

Enabling or disabling the PrintCryption-native solution

1. From the Embedded Web Server, click Network/Ports.
2. Click TCP/IP > TCP Port Access.
3. Select TCP 9198 (PrintCryption).

Automated certificate management

Markvision Enterprise

Certificates are used by the printer to establish a TLS, IPsec, or 802.1x connection and to identify other devices on the network securely. Printers can also use these certificates for LDAP over TLS authentication and address book lookups.

Certificate authorities (CA) are trusted servers that can issue various types of certificates on a network often tied to a directory or identity service. With Markvision Enterprise (MVE), administrators can easily manage device configurations, including certificates, on a fleet of network printers (scalable to thousands of devices).

Intuitive features such as the following make it easier to ensure security compliance across the enterprise:

- Managing firmware and settings
- Custom table views are exports
- Specified-time firmware updates
- Automatic certificate management

MVE supports the following certificate management protocols and platforms:

- **Enrollment over Secure Transport protocol (EST)**—The EST protocol is defined in RFC 7030 and standardizes an authenticated request and response exchange process with the CA. This process makes it more secure, faster, and easier for IT teams to deploy certificates on systems and devices than manually communicating the required information.

MVE supports the following EST authentication modes:

  - Client Certificate Authentication
  - Username and Password Authentication

- Microsoft certificate authority (CA) with multiple templates—Creating device certificates manually can be time-consuming. MVE integrates with your Microsoft certificate authority to create automatically, install, and verify the validity of a certificate. Renewal of certificates pending expiration is also automatically handled. MVE supports Microsoft Certificate Enrollment Web Services (MSCEWS) for interfacing with Microsoft CA services.
- OpenXPKI CA—OpenXPKI is an enterprise-grade PKI platform. It provides standard protocols and interfaces to operate a PKI in professional environments. It is primarily designed to run as an online Registration Authority (RA) or CA for managing X.509 certificates. But its flexibilities allow for a wide range of possible use cases regarding cryptographic key management. MVE supports EST, which is the recommended protocol when connecting to an OpenXPKI CA.
- Sectigo Certificate Manager - Sectigo Certificate Manager offers a reliable, consistent, automated approach for the entire certificate lifecycle management process. From discovery and provisioning to revocation, replacement, and renewal, and all the subtasks in between, the Sectigo CA agnostic platform allows you to manage all of these workflows in one place. MVE supports EST, which is the recommended protocol when connecting to the Sectigo Solution.

Unlike other print management solutions, MVE 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 MVE for free on its website. To download MVE, go to https://www.lexmark.com/markvision.

Native Held Jobs application

Overview

Native Held Jobs is an Embedded Solutions Framework (eSF) application that lets you hold jobs at the device until an authorized user releases them for printing. This way, it prevents the accidental exposure of sensitive or confidential business information.

Benefits

- Holds documents until they are released by an authorized user
- Releases print jobs whenever you are ready
- Reduces expenses related to print output
- Enables DRAM wiping of job data when enabled

Details

The Native Held Jobs application uses a four-digit PIN or an ID card to prevent unauthorized access to documents, keeping them safe and secure. This security feature helps stop sensitive company information from being left in the tray or picked up and viewed by an unauthorized person.

Users can send and store jobs in the printer and release them at their convenience. There is no need to interrupt what they are doing to pick up a document. Users can also review a document before printing multiple copies. They can also make sure that jobs are deleted after the documents are printed, and set up the job to print as many copies as necessary. Users can set jobs to expire at intervals ranging from one hour to one week. Also, by enabling the Clear Print Data setting, all DRAM that is used to store job data is automatically cleared after the job is completed.

By decreasing the amount of unclaimed documents left in the trays, companies can achieve significant cost savings while reducing exposure to unauthorized data disclosures.

Contactless and smart card authentication support

Overview

Lexmark devices support several different contactless card solutions for badge authentication where a user's identity is linked to their ID badge.

The badge authentication solutions verify the credential associated with the user's badge so that it can be used for the following:

- Accessing held print jobs
- Identifying the source of scanned documents
- Other identification purposes

Benefits

- Ease of use
- Use existing physical ID badges for logical access to the device
- Does not require a complete Active Directory PKI smart card infrastructure

Details

Lexmark badge authentication solutions are designed to work with card reader driver application solutions. The card reader driver solutions provide card ID data to other solutions that manage workflows or control access to device functions. For details, refer to the individual application solution descriptions.

Lexmark devices support several different card readers and card types, including products from the following:

- HID Global (Prox, iCLASS, and Indala)
- MIFARE
- Gemalto
- IDEMIA

The following readers are supported with the eSF keyboard reader application. Only the USB keyboard variant of these readers is supported. For supported card types of each reader, refer to the reader manufacturer specifications.

- Elatec TWN3
- Elatec TWN4
- rf IDEAS pcProx
- rf IDEAS pcProx Plus (RDR-80581AKU only)

Other keyboard emulation readers are supported on a per-customer basis when requested. Magnetic stripe cards are supported with the following readers (driver application not required):

- MagTek 21040102
- MagTek 21040107
- MagTek SureSwipe 21040145

CAC/PIV and SIPRNet card authentication

Overview

The Common Access Card (CAC) and Personal Identity Verification (PIV) authentication solution provides processes to control the security of networked Lexmark MFPs in federal government operations. The solution also supports SIPR tokens to provide access over the Secret Internet Protocol Router Network (SIPRNet).

Lexmark partners with 90Meter to implement the benefits of smart card security. This solution is embedded directly into the Lexmark device firmware, giving users a familiar printer authentication experience that closely resembles their workstation authentication workflow. The 90Meter solution delivers advanced document encryption, cryptographic signature functionality, and authoritative use of identity credentials. The solution also meets the U.S. federal government requirement for two-factor authentication and facilitates the use of PKI authentication tools.

Lexmark's partnership with 90Meter leverages many benefits of smart card security, including the following:

- The solution is embedded in firmware.

- Users experience as much security at the printer or MFP as at their own workstation.
- Ensures ongoing compatibility with SIPR tokens.
- Fulfills the latest government security mandates including FIPS 140-2 and FIPS-201.
- Advanced document encryption, cryptographic signature functionality, and authoritative use of identity credentials.
- Simultaneously supports multiple card types.

Benefits

- Delivers a flexible and easy configuration function for administrators
- Holds confidential print jobs until released by an authorized recipient
- Validates a card through Active Directory or Online Certificate Status Protocol (OCSP) for Tumbleweed or CoreStreet

Details

The Lexmark solution ensures that only authorized employees can access the network through its devices, giving government agencies another option for enhanced network security protection. Users cannot initiate workflow processes at locked devices without first inserting a CAC or SIPRNet card and obtaining authentication. Because the user's identification is associated with all functions initiated while the CAC or SIPRNet card is in the reader, an audit trail can also be created to track user activity.

Using the user's credentials from a CAC or SIPRNet card enhances the Scan to Email workflow by providing a more secure, personalized experience. Email addresses can be found without the need for a service account. Outgoing email is addressed with the user's account information, eliminating anonymous email. S/MIME support is available for enhanced security and privacy. CAC or SIPRNet credentials can be used to log in to an Exchange server through SMTP to validate user authorization before sending an email. The Lexmark CAC or SIPRNet solution has a rich set of customization capabilities so that only authorized users have access to specific workflows.

You can set up global restrictions so that CAC or SIPRNet authentication is required for scan and network functions, but not for print, copy, and fax. Users can also be organized by Active Directory groups so that function access is available only to authorized users.

The Lexmark CAC or SIPRNet solution for MFPs follows the same protocol as current laptop and PC CAC authentication processes. The onboard CAC or SIPRNet reader and user-friendly e-Task MFP touch screen makes authentication simple and secure.

Authentication process

1. Insert a CAC or SIPRNet card in the MFP card reader. The device prompts to enter a valid PIN.
2. The MFP validates the PIN against the CAC or SIPRNet card. It then extracts the PKI certificates from the CAC or SIPRNet card and sends them to the Windows domain controller for validation. The domain controller response can be validated at the MFP or against an OCSP responder or repeater.

3. When the card is validated, the MFP home screen appears, and user preferences and other system parameters are also implemented. You can then perform any of the following MFP functions:

- Scan to Email (digitally signed and encrypted).
- Scan to Home (or other network folder).
- Scan to Document Management System

Leave the CAC or SIPRNet card in the reader if you want to require no additional login when performing more MFP functions. A user remains logged in if the CAC or SIPRNet card stays in the reader. Removing the card returns the MFP to its locked, secure state.

Note: Lexmark PIV authentication meets all current Homeland Security Presidential Directive-12 (HSPD-12) standards.

Lexmark Contact Authentication Device

Overview

The Lexmark Contact Authentication Device provides enhanced control access to network printers and MFPs with secure authentication at print release. The device easily connects on the front of the printer or MFP and instantly provides a more secure environment for your business. The carefully engineered features of the device enhance security and prevent unauthorized users from gaining access to sensitive information.

With a single touch, administrators can use the Lexmark Contact Authentication Device to manage access to devices and authorize access to specific functions including e-mail, fax, copy, or scan. Plus, the device provides full compliance with all major industry standards and works seamlessly with virtually every contact smart card.

Lexmark Secure Document Monitor

Overview

In today's digital world, most security efforts are focused on preventing external threats. But what about the malicious and non-malicious breaches that are occurring internally? As information is shared and accessed across a growing number of sources, the potential for insider threats is growing in scope and complexity. That risk is especially present with sensitive hard-copy documents that are accessed, shared, or received from

printers and MFP. Lexmark Secure Document Monitor (LSDM) lets you monitor hard-copy data for increased

visibility, making it easier to investigate incidents, protect data, and prevent costly breaches.

Improper document security leads to the following:

- Regulatory fines, disclosure of trade secrets, and negative impact to reputation and stock price
- Potentially catastrophic risk of customer loss due to private information leaks and exposure to cyber theft

According to the Ponemon 2022 Cost of Insider Threats Global Report, organizations are reporting a steep increase in insider threat incidents, year over year. The average incident cost now at $15.4 million.

Every security organization within a company aims to protect their digital assets, devices, and services from being disrupted, stolen, or exploited by unauthorized users.

LSDM can help fill the hard-copy monitoring gap. It resides in an organization's Lexmark MFP to capture content and user data automatically and discreetly from every document that passes through. It allows for capture that is happening in real time, without interrupting or delaying processes and performance. From there, the captured

data is routed seamlessly to the Data Loss Prevention (DLP) or monitoring system in the organization. LSDM is flexible enough to integrate with existing security solutions or homegrown systems. For a more robust end-to-end monitoring and protection platform, Lexmark can provide a bundled offering, including LSDM and risk management solutions from innerActiv.

Benefits

- Tracks every document that is printed, copied, scanned, or faxed through a supported Lexmark MFP
- Audits and monitors previously inaccessible information to check for leaks
- Helps facilitate compliance with government and industry regulations
- Adds powerful monitoring capabilities to the system at a lower cost

Details

LSDM creates a searchable digital image file of every document that passes through the supported Lexmark MFP. This file includes print jobs that you send from your computer or mobile device, documents that are scanned or copied, and incoming and outbound faxes.

These digital images are stored with related metadata, such as device, user, and location, preparing them for document auditing. LSDM lets you launch forensic searches based on keywords or phrases (full text search) and document attributes (who, what, when, and where the event occurred). You can even search text in graphics, illustrations, and photos. With the Discovery Alerts feature, which continuously searches content as it passes through the system, you are automatically notified if any keywords or phrases are found.

Share data with Lexmark

At Lexmark, we are committed to delivering the best possible experience for our customers and always look for opportunities to improve our award-winning product line.

We rely on customer and device feedback to make our products the best that they can be. This feedback helps us understand key device performance metrics to help us drive future innovations in product design and service.

Sending information to Lexmark is a simple and easy way to provide feedback. However, no information is sent to Lexmark unless you give Lexmark permission to do so. If you choose to participate, then your device periodically sends Lexmark an anonymous summary of the following, depending upon which information you choose to share:

- Device usage
- Performance information

Information is sent to Lexmark over your Internet connection. You can choose to start or stop sending information at any time. Different printer models and different firmware versions can send different types of information.

The following are the two types of information:

- Supplies and page usage information, such as the number of pages and toner levels. This information helps Lexmark better understand how customers use our products.
- Device performance information, such as device errors and metrics. This information helps Lexmark understand device performance and enable a higher level of service.

Services

Lexmark Security Services

Lexmark provides next-level print security by offering the following professional services:

- Security consulting—Helps customers identify and address general print security.
- Security assessment—Identifies risks, vulnerabilities, and security improvements specific to their fleet of Lexmark devices.
- Configuration management—Protects printing and scanning ecosystems with managed standardization and ongoing monitoring provided by Lexmark.

Security consulting

Lexmark's security consultants depend on our deep industry knowledge to help customers understand and identify potential security concerns within their print environment. They can advise on relevant device settings and configurations, along with critical components such as print drivers and print-related infrastructure. In addition, Lexmark goes beyond the technical aspects by offering focused security training for IT security and staff. By fostering a culture of security consciousness through knowledge, Lexmark can strengthen the overall security posture of your organization.

Security assessment

Discover security concerns across your printing and scanning fleet with regularly scheduled assessments to detect and report on the risks associated with your Lexmark devices.

By leveraging this set of data-driven analysis services, organizations can elevate the overall security profile of your Lexmark environment by doing the following:

- Understand where the threats are in your print fleet today.
- Build a tailored secure configuration baseline with remediation recommendations.

Configuration management

Lexmark manages printer configurations including device settings, firmware revisions, and other installations and updates for all your Lexmark devices. Lexmark proactively monitors configurations and restores them if a device falls out of conformance with its custom configurations. This way, Lexmark increases security and reduces the device management burden on your IT team.

Using Lexmark's broad set of cloud- and premise-based device management capabilities, ongoing monitoring and configuration conformance keeps security issues addressed in a timely manner. Lexmark also works quickly to deploy updates as Common Vulnerabilities and Exposures (CVE) are discovered. As a result, your devices maintain functionality, security, and uptime so your users can stay focused on critical, value-added work. For more information on Lexmark Security Services, go to **https://www.lexmark.com/en_us/services/managed-print-services/mps-security-services.html.**

Standards

Overview

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

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.

For more information, go to https://www.lexmark.com/security.

You can also refer to the Lexmark Security Reference Guide at

https://media.lexmark.com/www/idml/assets/asset_17072/media/en_US/pdfs/low.pdf.

Common Criteria (NIAP/CCEVS Certification, ISO 15408)

Overview

Common Criteria represents a framework to provide a validation of the security functionality of a computer system. By performing a set of rigorous and repeatable tests, the framework provides participating countries assurance that the product meets the internationally agreed-upon security functional criteria. By meeting the requirements defined in the Common Criteria framework, a product evaluated by one nation is considered to have a valid evaluation by all other nations who have signed the Common Criteria Recognition Arrangement (CCRA). This, in practice, can result in common procurement requirements for the governments that are part of the CCRA.

Benefits

- 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).
- Two separate validations are performed on Lexmark devices: one with a hard drive and one without a hard drive.

Details

Lexmark 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). Lexmark will have devices cross listed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL).

In some cases, Lexmark may have two or more separate evaluations listed with similar model numbers. This is done because some Lexmark devices ship with a hard drive or have other functional differences, which require additional security targets to validate the security capabilities of the device. Adding these other validated devices gives Lexmark customers more options when selecting the appropriate device that meets their internal security requirements.

Federal Information Processing Standards (FIPS)

Overview

FIPS is a standardization developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors. The 140 series of FIPS are U.S. government computer security standards that specify requirements for cryptographic modules.

The FIPS 140 Publication Series is issued by the National Institute of Standards and Technology (NIST) to outline the requirements and standards for cryptographic modules. The FIIPS include both hardware and software components that are used by departments and agencies of the United States federal government. The FIPS 140 standard is an outline of requirements that can be used to provide the necessary conditions to secure information. But these requirements are not, and must not be, a guarantee of information security. The requirements covered within the FIPS 140 publication are specific to documented cryptographic modules and, sometimes, source code around the module.

Benefits

- Third-party validation assures customers that the algorithm and module meet the requirements as outlined by FIPS.
- Validation ensures that data stored in a device hard disk is secured through a FIPS standard protection mechanism.

Details

Lexmark has also completed a FIPS 197 Cryptographic Algorithm Validation Program (CAVP) on the Lexmark devices. This validation provides further assurance of the security of user data while in transit and at rest on Common Criteria-validated devices. CAVP allows for independent validation of the correct implementation of cryptographic algorithms that are used within Lexmark devices.

Lexmark validates not only the algorithm used to secure information on the device but also the cryptographic module through NIST's Cryptographic Module Validation Program (CMVP).

- CMVP validates the use of cryptographic modules as outlined in FIPS 140-2 for the encryption of all data that has a classification of Sensitive But Unclassified (SBU) or above. Lexmark FIPS 140-2 certification will be sunset on March 8, 2026.
- 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.

ISO 27001 Information Security Management System Certification

Overview

Lexmark has obtained the ISO 27001 certification for the people, processes, and technology supporting the development, operations, and infrastructure underlying its worldwide Managed Print Services (MPS) and Lexmark Cloud Services (LCS) offerings. 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.

ISO 20243 Supply Chain Certification

Overview

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 associated 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.

SOC 2 Type II for Lexmark Cloud Services

Lexmark's unique industry position as an end-to-end technology owner is what enables this seamless device-to-backend system connectivity. From the print engine to device communication, to its single global IoT system, Lexmark leverages advanced technology architecture that delivers a truly integrated connectivity solution.

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 with whom we have an active nondisclosure agreement (NDA). SOC 2 is developed by the American Institute of Certified Public Accountants (AICPA). It defines criteria for managing customer data based on five "trust service principles": security, availability, processing integrity, confidentiality, and privacy.

For more information on Lexmark device certifications, see

https://www.lexmark.com/en_us/solutions/security/device-certifications.html.

Notices

March 2026

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user's responsibility.

For Lexmark technical support, go to **http://support.lexmark.com.**

For information on Lexmark's privacy policy governing the use of this product, go to **www.lexmark.com/privacy.**

For information on supplies and downloads, go to **www.lexmark.com.**

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48

C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

26WWM13805

Trademarks

Lexmark, the Lexmark logo, Markvision, and PrintCryption are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Android is a trademark of Google LLC.

Microsoft, Active Directory, and Windows are trademarks of the Microsoft group of companies.

PCL® is a registered trademark of the Hewlett-Packard Company. PCL is Hewlett-Packard Company's designation of a set of printer commands (language) and functions included in its printer products. This printer is intended to be compatible with the PCL language. This means the printer recognizes PCL commands used in various application programs, and that the printer emulates the functions corresponding to the commands.

PostScript is either a registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries.

Wi-Fi® is a registered trademark of Wi-Fi Alliance®.

All other trademarks are the property of their respective owners.

Index

26WWM13805

26WWM13805