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

Our devices provide high-end features that protect your corporate documents and data throughout your workflow—from the data traveling through your network to the pages landing in your output tray.

This reference guide explains our security features and benefits—and discusses these four security areas that help protect your user data and device:

- Secure remote management
- Secure network interfaces
- Secure access
- Secure data

Learn how easy it can be to lock down network-facing devices, plus securely access and remotely manage them. Whether you’re swapping machines or adding to your fleet, you can easily configure your security features—which come standard and embedded in our firmware—and implement them in the way that’s best for your organization. Please refer to the Lexmark Security Features table for a comparison of printer models and features.

**Secure Remote Management**

**Manage devices securely and efficiently**

To meet the demands of efficiently managing a fleet of networked printers, Lexmark’s solutions-capable devices have the remote management security features you need—allowing only authorized personnel to configure the device for network access.

Plus, these features are designed to protect network traffic associated with remote management to prevent information from being captured, stolen or abused. And all features can be configured through the device’s embedded Web page.

**Audit Logging:** By enabling Audit Logging, Lexmark devices can track security-related events with features that track device setting changes and export these into detailed logs describing system, user or activity events. The event tracking feature proactively tracks and identifies potential risks and integrates with your intrusion-detection system for real-time tracking.

**Digitally Signed Firmware Updates:** You can also protect your device from malicious software. Our solutions-capable printers and MFPs automatically inspect downloaded firmware upgrades for the appropriate Lexmark digital signatures. Firmware that is not authenticated and/or signed by Lexmark is rejected to safeguard your device from malicious software, viruses and worms.

**Certificate Management:** Our printers and MFPs use certificates for HTTPS, SSL/TLS, IPSec and 802.1x authentications. Since they easily integrate with a public key infrastructure (PKI) environment, these devices can set up trusted communication transportation for 802.1x, IPSec, certificate authorization for validating domain controller.
certificates, EWS and LDAP SSL or any other service that uses Secure Sockets Layer (SSL) or Transport Security Layer (TLS).

**HTTPS:** You can securely manage your networked printers and MFPs with HTTPS from the device’s embedded Web page. For more security, utilize HTTPS to conveniently and effectively manage the device remotely.

**SNMPv3:** Lexmark solutions-capable printers and MFPs support SNMPv3 (Standard Network Management Protocol, Version 3). This protocol features extensive security capabilities, including the authentication and data-encryption components for the secure remote management of a device. SNMPv1 and SNMPv2 are also supported.

**Secure Password Reset:** You can reset the access control setting on the device’s security menu when an administrative password is lost or forgotten, or when the device loses network connectivity. Just go to a firmware setting on the device’s embedded Web page and adjust a jumper on the device system board.

**Secure Network Interfaces**

**Protect devices from hackers and viruses**

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 interfaces 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 a device—no further purchases necessary.

**TCP Connection Filtering:** Solutions-capable printers and MFPs can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses also known as whitelisting. This disallows all TCP connections from other addresses, protecting the device against unauthorized printing and configuration.

**Port Filtering:** You can gain more control over your network device’s activity with port filtering, which allows you to easily configure your device to filter out traffic on specific network ports. Protocols such as telnet, FTP, SNMP, HTTP and many others can be disabled.

**802.1x:** 802.1x port authentication allows printers and MFPs to join wired and wireless networks by requiring authentication. You also have WPA Enterprise security support when you use 802.1x port authentication with the Wi-Fi Protected Access feature of an optional wireless print server.

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

**Secure NTP:** Lexmark devices support the use of Secure Network Time Protocol (NTP), which is used for clock synchronization of various devices on the network. This complements audit logging to prevent date and time changes.

**Fax/Network Separation:** In security-conscious network environments, combining both network and fax modems on a single device may be a concern. Lexmark designs MFPs so that any interaction between the modem and network adapter is prevented. The modem only accepts image data from a fax transmission. Any other data, remote access, executable code or firmware updates are declared invalid and will terminate the telephone connection to keep your fax secure.

Continued on next page
Secure Access
Make everyday operations simple and safe

Network scans and printed documents which routinely contain sensitive information—such as financial data, customer or employee identification and account information—are often overlooked when it comes to network security. Lexmark devices include standard features that can substantially reduce this security risk.

Authentication and Authorization: You can restrict device functions so that users must authenticate prior to accessing them. You can also configure the device to authenticate and authorize users against internal accounts, passwords and/or PINs—and against a corporate directory via NTLM, Kerberos 5, LDAP and/or LDAP+GSSAPI. These authentication methods are secure over an SSL channel and are compatible with Active Directory and other directory-server platforms.

Active Directory: Support for Active Directory can be found on many of our easy-to-use touch screens, allowing you to manage efficiently your security configurations on a device. Your Active Directory authentication is provided by Kerberos and authorization is provided by LDAP+GSSAPI.

Protected USB Ports: Our USB host ports have various security features, including access restriction through authentication, file-type parameters, device-interaction scheduling, boot-support restriction and the ability to disable the USB host port completely.

Secure LDAP: All Lightweight Directory Access Protocol (LDAP) traffic to and from Lexmark devices can be secured with TLS/SSL to preserve its confidentiality and privacy. LDAP information that is exchanged over a TLS/SSL connection such as—credentials, names, email addresses and fax numbers—is encrypted.

Auto-Insertion of Sender’s Email Address: No more anonymous emails—recipients can now validate the sender. When a user authenticates in order to scan a document to email, the email address of the sender is automatically identified and inserted into the From field.

Security Templates: As a device administrator, you can use security templates to help restrict access. The templates appear in the Access Control drop-down menu, providing more control over important security settings.

Access Controls: With more than 50 Access Controls, choose from a list of available security templates to control local and remote access to specific menus, functions and workflows, even disable functions entirely.

Login Restrictions: You can prevent unauthorized use of a device by restricting the number of consecutive failed logins.

Operator Panel Lock: The Operator Panel Lock feature allows a device to be locked so that the operator panel cannot be accessed for operations or configuration. If the device has a hard disk, incoming print and fax jobs are stored on the hard disk instead of being printed. When you enter an authorized user’s credentials, the device unlocks and normal operation resumes, printing any held jobs.

Confidential Print: Print jobs are held in RAM or on the hard disk until the intended recipient enters the appropriate PIN and releases the job for printing. You can set held jobs to expire after an elapsed time—from one hour to one week. Plus, you can limit the number of times a PIN can be entered incorrectly before the job is purged.

Continued on next page
Incoming Fax Holding: Lexmark devices can be configured to hold rather than print incoming faxes during scheduled times. Incoming faxes are held securely on the hard disk until the proper credentials have been entered on the Lexmark device.

Secure Data
Encrypt, wipe and physically defend stored data

Lexmark equips some of its printers and multifunction devices with internal hard disks to store images of documents for job processing. These devices feature controls that help secure data when it is stored or passed through the hard disk—plus, they block malicious users from gaining physical access to the hard disk.

Hard Disk Encryption: You can encrypt the hard disks in your printer and MFPs. Lexmark uses the Advanced Encryption Standard (AES) with key lengths of 256 bits, which are internally generated by the device to encrypt all data on the hard disk.

Automatic Disk Wiping: This file-based disk wipe immediately sanitizes the hard disk after the job has been processed so that no residual data can be read. Lexmark devices offer a single-pass wipe or multi-pass wipe which are both compliant with National Institute of Standard Technology (NIST) and Department of Defense (DoD).

Out-of-Service Disk Wipe: Out-of-Service Disk Wiping should occur before a device leaves any current location. You can access the Wipe Disk feature through the device’s configuration menu to erase all contents of a disk. Two options are available: single-pass and multi-pass.

Physical Lock Support: Lexmark printers and MFPs support cabled computer locks that allow you to physically secure the devices’ critical and sensitive components such as the motherboard and hard disk.

Non-Volatile Memory Wipe: This tool erases all contents stored on the various forms of flash memory on your device. You can completely clear all settings, solutions and job data on the device. This feature is ideal when retiring, recycling or removing a device from a secure environment.

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