

# Security Is Only as Strong as the Weakest Link

## **TRIPLE LAYER SECURITY: Device, Document, Network**

Every link in the chain is critical: every access point and every connection; every protocol, setting, and function; every print, copy, and scan.

While it is the ransomware, the phishing schemes, the trojans and other malware attacks that get most of the attention, comprehensive data security is about more than network breaches and external bad actors. It's about the documents themselves, which when printed or scanned can get into the wrong hands, even accidentally. It's about restricting access to device functionality, to prevent unauthorized duplication or sharing.

Brother printers, all-in-ones, and scanners provide Triple Layer Security – protection at all three levels: device, document, and network.

**In partnership with**



# TRIPLE LAYER SECURITY: Device, Document, Network

<b>DEVICE SECURITY</b>	<small>PAGE</small> <b>03</b>
Password Intelligence	
Digitally Signed Firmware	
Setting Lock	
Secure Function Lock	
Integrated NFC Card Reader	
Active Directory Authentication	
LDAP Authentication	
Custom User Interface	
<i>Integrated Partner Solutions:</i>	
PaperCut MF	
Kofax ControlSuite	
uniFLOW	

<b>DOCUMENT SECURITY</b>	<small>PAGE</small> <b>06</b>
Secure Print Advanced	
Cloud Secure Print	
Scan to Network Folder (SMBv1,2,3)	
Scan to SSH Server (SFTP)	
Scan to Email Server	
Scan to SharePoint / SharePoint Online	
Scan to Secure PDF	
Scan to Signed PDF	
<i>Integrated Partner Solutions:</i>	
TrueSign	
DischargeRx by TroyRx	
PaperCut MF	
Kofax ControlSuite	
uniFLOW	

<b>NETWORK SECURITY</b>	<small>PAGE</small> <b>10</b>
HTTPS	
IPPS	
SMBv3 Scanning	
SNMPv3	
TLS Certificates	
Secure Email Certificate	
IPv4 Filter	
IPv6 Internet Protocol	
IEEE 802.1X	
IPSec (IP Security)	
Syslog Report	
BRAdmin Professional 4	





## DEVICE SECURITY

**Triple Layer Security begins at the device.** Who should have access? Which functions are available to which user? Brother printers, all-in-ones, and scanners can limit device access for certain groups or specific individuals, including restricting particular functions. Built-in security features can be complemented with easily integrated third-party solutions.

**Password Intelligence**

**Digitally Signed Firmware**

**Setting Lock**

**Secure Function Lock**

**Integrated NFC Card Reader**

**Active Directory Authentication**

**LDAP Authentication**

**Custom User Interface**

***Integrated Partner Solutions:***

**PaperCut MF**

**Kofax ControlSuite**

**uniFLOW**



# DEVICE SECURITY

## Password Intelligence

Device security starts with restricting access to the web-based administration of your machine. Brother recommends changing the default password to a new password between 8 and 32 characters, containing both uppercase and lowercase letters, numbers, and a special character. The maximum number of retries can be set from 1 to 50, after which there is a lockout time of up to 30 minutes.

**DID YOU KNOW?**  
Brother firmware is digitally signed to help prevent unauthorized firmware from being installed on the device. For added security, firmware updates can be disabled by the administrator.

**BEST FOR**  
Securing access to web-based management of the device.

## Setting Lock

Set a password so that only authorized users can change device settings. This ensures consistent and protected workflows, and helps prevent unauthorized sharing of confidential information.

**BEST FOR**  
Restricting who has permission to change device settings.

## Secure Function Lock

Restrict functions based on company risk protocols. Restrict printing (page limits, color printing) to help manage costs. Job Logging feature generates activity reports for specific groups or individual users.

**BEST FOR**  
Securing workflows and controlling costs – without the expense of management software, servers, or external card readers.

## Integrated NFC Card Reader

Authenticate users through built-in card reader (with Secure Function Lock) eliminating the cost of an external third-party card reader. Badges streamline the authentication process for network users and integrate easily into secure workflows.

**BEST FOR**  
Using badges for user authentication and accessing specific functions.

## HID Compatibility

Brother devices are also compatible with third-party HID readers, which can be integrated into an existing HID card authentication environment, or used to strengthen a new security policy. External card readers require third-party middleware.

Brother devices do not have a hard drive, eliminating the risk of stored information.

## Active Directory Authentication

Manage device access – including adding or removing users – from the Active Directory console, without making changes at the device itself. Assign specific destinations for scanned documents for each user with Send to My Folder or Send to My Email functions.

### DID YOU KNOW?

LDAP Authentication allows a network administrator to authenticate users and manage machine access to an existing LDAP Server.

### BEST FOR

Protecting important document workflows by requiring users to authenticate at the device before accessing device features.

## Custom User Interface

Modify the standard user interface with different icons, available device features, and backgrounds. Customize business workflows to allow access to specific device functions, while hiding others. Predefined icons reduce the risk of documents accidentally being sent to the wrong destination.

### BEST FOR

Streamlining workflows, enacting security policies, and branding the device display.

## INTEGRATED PARTNER SOLUTIONS



### PaperCut MF

Control all aspects of the printing environment, including security, rules-based printing, and job accounting. Integrates easily with Brother devices – no external release stations required.

### BEST FOR

Managing print accounting, print control, and secure release.



### Kofax ControlSuite

Easily manage document workflow, cost recovery, and storage across any combination of cloud or internal systems, technologies, and devices. Offered as an embedded solution on select Brother devices.

### BEST FOR

Applying security controls, tracking and monitoring compliance policies, and automating document management.



### uniFLOW

Establish printing rules for an entire fleet to optimize printing within the organization. Assign costs to a multi-level center, enabling chargeback to customers or projects.

### BEST FOR

Controlling costs, increasing document security, and improving print productivity.



## DOCUMENT SECURITY

**When a document is printed, who can retrieve it?** When a document is scanned, where can it be sent?

Brother offers a wide range of built-in document security features for printers, all-in-ones, and scanners. Brother devices are also compatible with many third-party document security solutions.

**Secure Print Advanced**

**Cloud Secure Print**

**Scan to Network Folder (SMBv1,2,3)**

**Scan to SSH Server (SFTP)**

**Scan to Email Server**

**Scan to SharePoint /  
SharePoint Online**

**Scan to Secure PDF**

**Scan to Signed PDF**

***Integrated Partner Solutions:***

**TrueSign**

**DischargeRx by TroyRx**

**PaperCut MF**

**Kofax ControlSuite**

**uniFLOW**



# DOCUMENT SECURITY

## Secure Print Advanced

Ensure sensitive documents print only upon user-authentication on many network-connected Brother devices (via PIN or via NFC card using an integrated NFC card reader). Meet document handling guidelines and regulations without the extra cost of IT services, middleware, or additional infrastructure.

With Secure Function Lock, add and remove users in a few simple steps, including setting associated NFC card identification and allowing access to certain device functions.

## Cloud Secure Print

Send sensitive documents to remote printers over the internet – without connecting to a corporate network, and without loading print drivers.

### BEST FOR

Securing printed documents on many network-connected devices.

## Scan to Network Folder (SMBv1,2,3)

Scan documents directly to a shared network folder without installing software on a local PC. Supports standard document storage and security practices (SMBv1/v2 can be disabled to meet security requirements).

### BEST FOR

Configuring one device as a shared resource to send scanned documents directly to a network folder.

## Scan to SSH Server (SFTP)

Establish a private and safe data stream (Secure Shell File Transfer Protocol) when scanning to a network destination. Delivers end-to-end security based on RSA encryption and Public Key Authentication.

### BEST FOR

Scanning documents securely to a network or cloud destination.

## Scan to Email Server

Scan documents directly to recipients via email, without a PC. Access recipient addresses from the device's address book or from the corporate address book via Active Directory or LDAP.

### BEST FOR

Configuring one device as a shared resource to send scanned documents directly to an email server.



## Scan to SharePoint / SharePoint Online

Scan documents directly to a Microsoft SharePoint server. This cost-effective solution does not require additional middleware.

### BEST FOR

Scanning documents directly into SharePoint workflows.

## Scan to Secure PDF

Add PIN protection to the file during the scanning process. This solution encrypts the PDF document, which then can be accessed only if the PIN is used.

## Scan to Signed PDF

Include a digital certificate within the document to help prevent data-tampering and author-impersonation. The digital certificate uses the security feature of a PDF application to determine whether a document has been modified or the original author has been changed.

### BEST FOR

Authenticating content and authorship of documents in various PDF formats.

Brother “scan to” solutions support common formats: JPEG, TIFF, PDF (multi- and single-page), PDF/A, Secure PDF, Signed PDF, XPS



## INTEGRATED PARTNER SOLUTIONS



### TrueSign

Scan documents directly into TrueSign, from Brother devices supporting Easy Scan to Email. TrueSign is a legally recognized electronic signing platform that enables users to create, sign, share, and submit documents from a single dashboard. As a cloud application, TrueSign integrates directly into an organization's business processes.

**BEST FOR**  
Secure e-signing of contracts, HR documents, court orders, and more.



### DischargeRx by TroyRx

Print state-compliant and federal-compliant prescriptions directly onto plain paper from Brother devices, avoiding the risk of theft of preprinted forms. Meet CMS security requirements and protect against fraud, alteration, and falsification. This solution also has a full reporting suite for tracking how many prescriptions have been printed, by who, and at what locations.

**BEST FOR**  
Printing tamper-resistant scripts on plain paper.



### PaperCut MF

Control all aspects of the printing environment, including security, rules-based printing, and job accounting. Integrates easily with Brother devices – no external release stations are required – and can be used with a built-in NFC card reader on select Brother devices.

**BEST FOR**  
Managing print accounting, print control, and secure release.



### Kofax ControlSuite

Easily manage, secure, and govern virtually every aspect of document information and distribution. Offered as an embedded solution on select Brother devices.

**BEST FOR**  
Managing all aspects of printing and document security.



### uniFLOW

Enable secure print job-release from any network printer. Print jobs follow the user from device to device to ensure the correct requested output.

**BEST FOR**  
Ensuring document security, even as users print to different devices.



## NETWORK SECURITY

**Ransomware, phishing schemes, trojans, malware, and more.** Protecting your network from external bad actors is foundational to every organization's security plan. In fact, unsecure printers are often hackers' favorite access points.

Brother devices feature the latest protocols, and can be easily configured to meet the demands of your unique security policies. When combined with monitoring and management capabilities, Brother helps ensure your network security is up to date.

**HTTPS**

**IPPS**

**SMBv3 Scanning**

**SNMPv3**

**TLS Certificates**

**Secure Email Certificate**

**IPv4 Filter**

**IPv6 Internet Protocol**

**IEEE 802.1X**

**IPSec (IP Security)**

**Syslog Report**

**BRAdmin Professional 4**



# NETWORK SECURITY

## HTTPS

Hypertext Transfer Protocol Secure is the foundation of secure data exchange on the web. All communications involving the device are encrypted to/from the email server, cloud-based services, Cloud Secure Print, and browsers, as well as the device's internal web-based management.

### BEST FOR

Securing communication between a web server and a web browser.

## IPPS

Print securely over the internet. Internet Printing Protocol uses TLS to communicate between the client and the printer, encrypting the document content, which ensures the privacy of documents sent across a network.

### BEST FOR

Printing securely over the internet.

## SMBv3 Scanning

Connect Windows clients and servers for secure shared access to scanned files. An SMBv3 file share configured with SMB encryption removes the need for a more complex IPSec configuration. The Brother embedded SMBv3 client supports:

- SMB Encryption (AES-CCM)
- Signing (AES-CMAC)

Supported file formats include JPEG, TIFF, PDF (multi- and single-page), PDF/A, Secure PDF, Signed PDF, XPS

### BEST FOR

Transmitting scanned data securely across untrusted networks.

## SNMPv3

Configure and manage networked devices securely. Simple Network Management Protocol enables user-authentication and data encryption.

### BEST FOR

Managing networked devices securely.



## TLS Certificates

Protect the transfer of data and information through an encrypted channel. Brother offers several TLS-based solutions, including TLS certificates for:

- 802.1X
- HTTPS Device Management
- Scan to Signed PDF
- Secure Scan to Email Server

### BEST FOR

Securing data on the network.

## Secure Email Certificate

Communicate directly with a secure email server using TLS v1.2, STARTTLS, and SMTP-AUTH. This solution offers password authentication, as well as encrypted data transmission using certificate-based TLS protocol.

### BEST FOR

Securely accessing either on-premises or cloud-based email servers.

## IPv4 Filter

Control device access for printing, scanning, and web-based management – either from a specific IP address or from several IP addresses by using a subnet mask.

### DID YOU KNOW?

For greater IP address security, Brother also supports IPv6.

### BEST FOR

Controlling access to the device for printing, scanning, and web-based management.

## IEEE 802.1X

Define a protocol that restricts unauthorized users from connecting to a LAN/WLAN through publicly accessible ports. Devices are secured on a network running enterprise authentication EAP-TLS with a security certificate from a RADIUS server.

### BEST FOR

Conforming to security policies and standards such as PCI Security Standards Council.

## IPSec (IP Security)

Ensure the integrity, confidentiality, and authentication of data communications over an IP network. This suite of protocols maintains secure tunnels and encrypts all data carried over the network. IP Filtering controls the IP addresses that can access the device.

### BEST FOR

Ensuring security of data communications over an IP network.



## SYSLOG Report

Send reports about network device events to a logging server running a Security Information and Event Management (SIEM) application, such as Splunk. Administrators often use SIEM applications to receive alerts on security risks from devices on the network.

### BEST FOR

Monitoring network devices using a SIEM application.

## BRAdmin Professional 4

View the status and activity of all networked printers supporting SNMP (v1,v2c,v3) via a single console, with a single login. Configure multiple devices at once, obtain setting data from an existing device, or create setting data using the Mass Deployment Tool, and apply it to many devices – including different models. Manage security settings and task automation through one central location.

- Configure device settings: network, location, contact, password, etc.
- Push security settings to the fleet
- Mass deploy settings in JSON/XML format
- Log file to an SMB network folder
- View device status
- Establish notifications and email reports
- Automated and scheduled device configuration
- Send file

### DID YOU KNOW?

For cloud management of devices, BRAdmin Professional 4 supports Microsoft Azure.

### BEST FOR

Managing and deploying network-connected devices from one central location.



## **AT YOUR COMPANY...**

**What are the needs for device security?  
For document security?**

**Are there security protocols for users?  
Are those protocols followed?**

**How old are most devices?  
How old is the oldest device?**

**How many different models?  
From how many different manufacturers?**

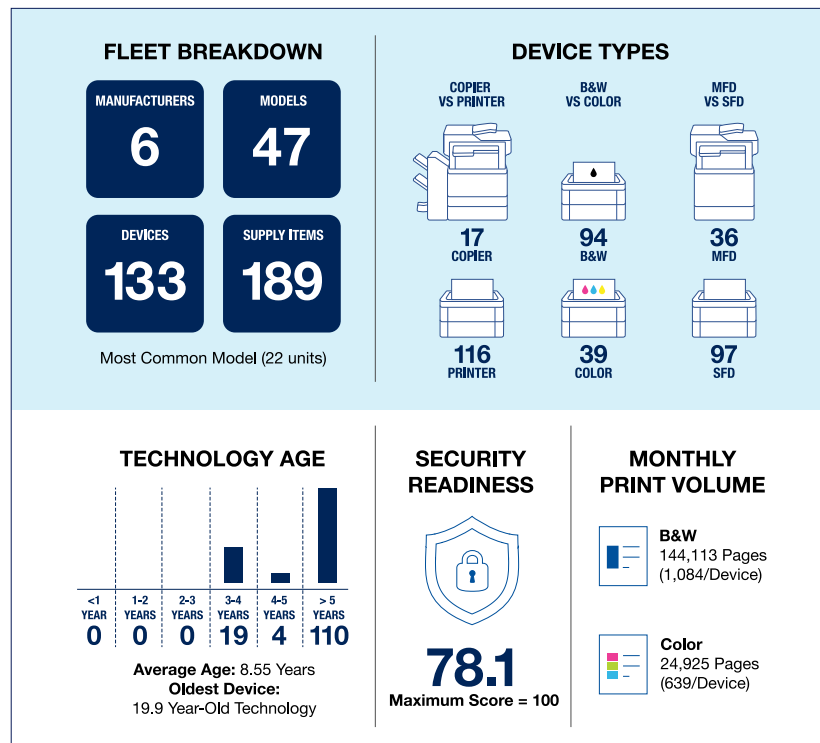
**Have default passwords been reset?**

**Are your network printers secure?  
What about for WFH employees?**

# A Predictive Assessment by Brother

This structured, no-cost examination can identify opportunities to improve security, maximize efficiency, and reduce cost. Is that worth an initial conversation? You tell us.

Example of a partial assessment report. For illustrative purposes only.



To learn more about Brother Predictive Fleet Assessments, please scan the QR code or contact us directly at:

[www.brother-usa.com/bmgcontactarep](http://www.brother-usa.com/bmgcontactarep)



©2023 BROTHER INTERNATIONAL CORPORATION

All trademarks and registered trademarks referenced herein are the property of their respective companies. Custom User Interface solution requires minimum purchase of ten printer/scanner units and purchase of professional services for development. PaperCut MF, Kofax ControlSuite, uniFLOW, TrueSign, and DischargeRx by TroyRx are third-party products and Brother International Corporation makes no representations or warranties regarding such product. Splunk is a registered trademark of Splunk Inc. in the United States and other countries. Images are for illustrative purposes only. All specifications subject to change without notice.