SECURITY HIGHLIGHTS

HELP PROTECT YOUR PRINT ENVIRONMENT

With confidential data regularly moving on a desktop, mobile device, and printer/MFP, it's important to help protect the print environment. Canon's imageCLASS printers and MFPs offer a wide variety of security features that can provide a layer of protection to help facilitate the confidentiality, accessibility, and availability of sensitive information.*

DEVICE SECURITY FEATURES

Canon imageCLASS devices can authenticate through standard Department ID Management or the optional uniFLOW (server-based or cloud-based) solution so only approved users can access the device and its functions. Both features can control device access, restrict function use, and oversee usage behavior. uniFLOW is implemented at the fleet level and offers users to log in via a PIN or an HID card. It can also be used to restrict unauthorized access; set user- and job-level rules; and deliver rich, real-time reporting insights to enable better control. Verify System at Startup is a process to help verify the validity of the device firmware and Application Library from unauthorized modifications.

DOCUMENT SECURITY FEATURES

Canon offers many ways to help limit access to documents managed by Canon hardware and software technologies, including Secure Print and Pull-Print,** Send-to-Myself Only, Fax Forwarding, and Fax Destination confirmation.

DATA SECURITY FEATURES

Canon imageCLASS devices don't have a built-in hard disk drive (HDD); this helps ensure that print job data is only stored in short-term memory and is automatically deleted when the job is complete, device power is shut off, or the job times out. This greatly minimizes the risk of critical data loss at the printer.

NETWORK SECURITY FEATURES

Standard network security features include the ability to set up the device to allow only authorized users and groups to access and print to the device. This helps limit device communications to designated IP/MAC addresses and controls the availability of individual network protocols and ports. Canon imageCLASS devices offer IPSec, a protocol for facilitating the security of IP packets sent and received over an IP network by helping to protect from threats such as theft, modification, and impersonation. The Wireless LAN is IPv6 compliant and supports the latest wireless encryption standards, including WEP, WPA, and WPA2.

* Not all features discussed are supported on all models and some features are optional. Please see page two of this document for features available by model.

** Pull-print requires uniFLOW. Check page two for compatible models.

SECURITY FEATURES	MF746Cdw	MF543dw	MF449dw	LBP352dn	LBP351dn	LBP325dn	LBP228dw	LBP712Cdn	LBP664Cdw
PRODUCTS									

DEVICE SECURITY (AUTHENTICATION)									
Device-Based Authentication (Department ID)	Standard								
Device-Level Log-in (Administrator)	Standard								
Server-Based Authentication (uniFLOW)	Optional								
Cloud-Based Authentication (uniFLOW Online)	Optional			N/A			Optional	N/A	Optional
Verify System at Startup	Standard			N/A			Standard	N/A	Standard
DOCUMENT SECURITY									
Encrypted Secure Print	N/A			Optional			N/A	Optional	N/A
Send to Myself (Only)	Standard		N/A						
Encrypted PDF	Optional		N/A						
Digital Signature PDF	Optional		N/A						
Fax Forwarding	Standard		N/A						
Fax Destination Confirmation	Standard		N/A						
DATA SECURITY									
No Hard Drive	Standard								
NETWORK SECURITY									
IP/MAC Address Filtering	Standard								
Port Filtering	Standard								
TLS Version Selection	Standard			N/A			Standard	N/A	Standard
TLS Encryption	Standard (1.0, 1.1, 1.2)								
USB Block	Standard (Device)			Standard (Device, Host)			Standard (Device)	Standard (Device, Host)	Standard (Device)
Destination Restriction	Standard		N/A						
IPSec	Standard								
IEEE802.1x	Standard								
MAIL SERVER SECURITY									
POP Authentication Before SMTP	Standard		N/A						
SMTP Authentication	Standard		N/A						

Canon
SEE IMPOSSIBLE