SMARTSHIELD

Integrated Printing Security Technology

For ColorWave and PlotWave printers

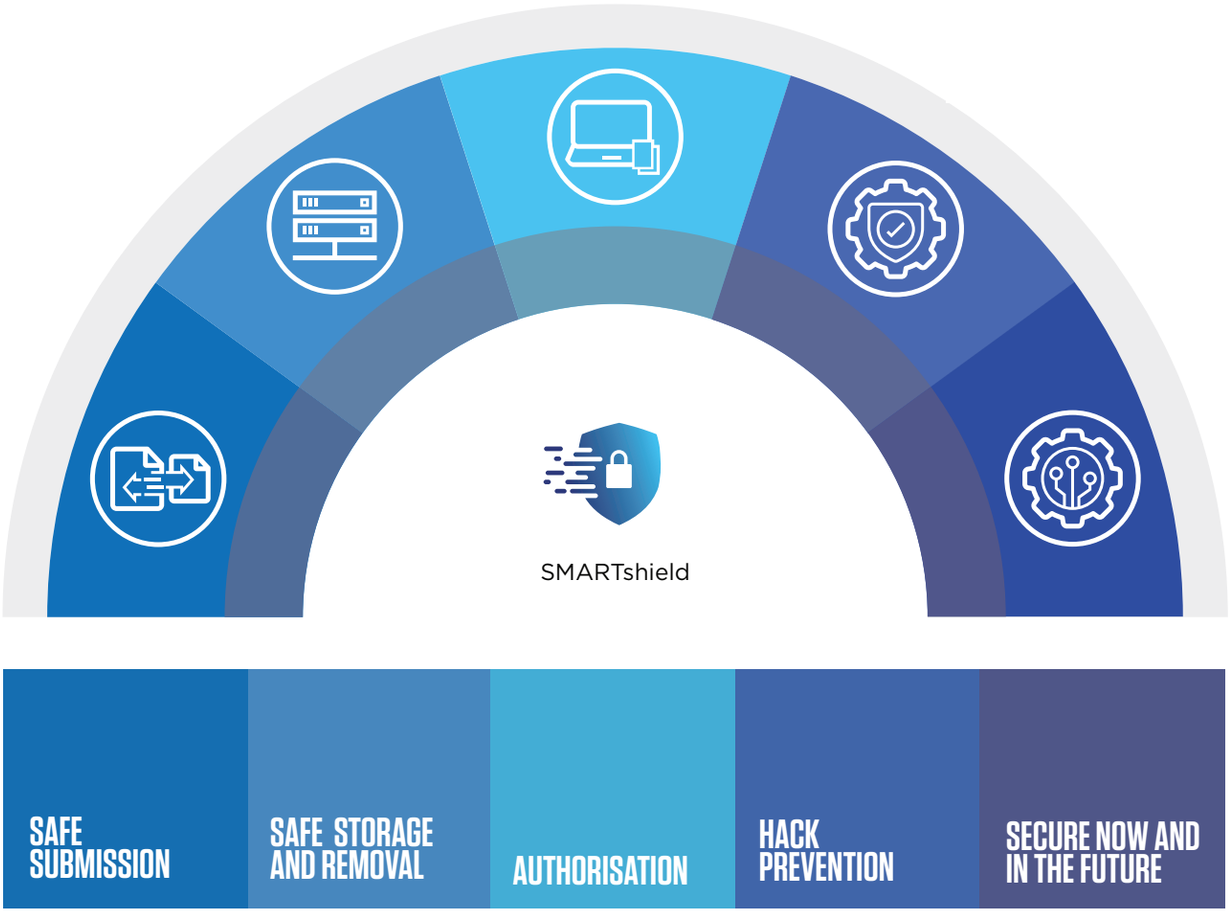
Canon

Delighting You Always

FIRST-CLASS PRINTING SECURITY

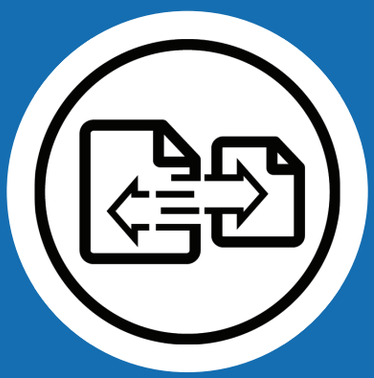
Our market-leading Wide Format printers address the security concerns of technical document users who handle confidential customer data.

SMARTshield is a suite of security features embedded in the total print workflow of the latest PlotWave and ColorWave systems. Designed to keep your systems safe: today and in the future.



Businesses and government organisations with Wide Format printers have the need to protect important, confidential, and sensitive information in the office and on networks. This includes information sent from individual workstations, other devices and data stored in the printer. It is also essential that systems are protected against any unauthorised access to confidential data and information. Every organisation needs a secure Wide Format printer for a hassle-free and safe print environment.

SMARTshield is a fully integrated printing security technology that is embedded in all our Wide Format Printers. SMARTshield features multiple security measures designed to keep data and information safe. With SMARTshield, all your security risks in every stage of the workflow process are addressed. SMARTshield secures you now and in the future.



SAFE SUBMISSION

Protect data while sending files to your printer – from any device.

Thanks to ClearConnect workflow applications, users can submit files from their desktop or any mobile device. With this level of flexibility and mobile access, it is essential that valuable data is submitted securely to the printer at all times.

- Internet Protocol Security (IPSec) compatibility
- IPv6 and IPv4 compatibility
- HTTPS

SMARTshield

SAFE STORAGE AND REMOVAL

Protect confidential data stored on the hard drive of the printer.

It is important to protect confidential data stored in the printer from being stolen or accidentally leaked from the company or department. SMARTshield encrypts data and restricts access with user identification to make sure your data is kept safe. By erasing data correctly, users can be ensured that confidential files are kept safely from unauthorised colleagues.

- Secure File Erase
- E-Shredding
- Removable hard disk
- Secure Boot
- Data encryption
- HDD destruction at the end of the contract

SMARTshield

AUTHORISATION

SMARTshield user authorisation restricts access to confidential files for unauthorised users.

By requiring users to authenticate, you can keep a tighter control of their activities. It is possible to limit the features and protocols that users can access and also, monitor the expenses incurred for each user.

- Control panel access lock
- Secure printing via domain credentials (Active directory)
- Secure printing via smartcard (excl. reader)
- Print files only available in your Smart inbox
- Scan to your personal home folder
- Print from your personal home folder
- Disable ports and interfaces
- Third-party software such as uniflow

SMARTshield

HACK PREVENTION

One of the greatest security challenges for any business is keeping hackers away. It is essential to restrict access to the printer and data stored on the controller (or hard drive).

SMARTshield addresses the challenge of hack prevention on a number of fronts:

- Disabling unused protocols
- SNMP v3
- IEEE 802.1x compatibility
- McAfee antivirus (optional)
- McAfee Whitelisting Application control (optional)

SMARTshield

SECURE NOW AND IN THE FUTURE

Hackers are constantly trying to find new ways to access your valuable information. SMARTshield has been designed to keep your information secure: today and in the future.

Our security specialists are constantly monitoring the latest risks to help ensure your data and your printers are secure. Current features include:

- Windows 10 IoT Enterprise LTSC controller software
- Support at least up to 2029 or beyond
- Remote controller security updates
- On Remote service

We understand your security concerns and have put in place a suite of features to address the risks that your business faces at every stage of the workflow process. Not just today, but also in the future.

SMARTshield

SMARTSHIELD COMPATIBLE

SMARTshield is integrated in the following systems:

ColorWave 3800

PlotWave 3500 Series

PlotWave 5000 Series

PlotWave 7500

SMARTSHIELD IN DETAIL

SAFE SUBMISSION

Internet Protocol Security (IPsec) compatibility	IPsec is a protocol that provides authentication, data confidentiality and integrity in the network communication between the controller and other devices.
IPv6 and IPv4 compatibility	Internet Protocol version 4 (IPv4) is one of the core protocols of standards-based inter networking methods in the Internet and other packet-switched networks. It uses 32 bit addresses. IPv6 is the most recent version and uses 128 bit addresses.
HTTPS	The HTTPS protocol is a more secure option to protect the network traffic for WebTools Express, Publisher Express and Publisher Select from being intercepted. Trusted certificates from a Certificate Authority can also be embedded in the controller to prevent a man-in-the-middle attack, where a malicious party plans to hack into the controller server.

SAFE STORAGE AND REMOVAL

Secure file erase	Automatically removes print, scan and copy jobs from the smart Inbox after the user defined time. The files erase is secure when enabling E-Shredding.
E-shredding	The e-shredding feature is a security feature which allows the system to overwrite any user print/copy/scan data after it has been deleted from the system. This feature prevents the recovery of any deleted user data including file content and file attributes, for instance if the disk is stolen.
Removable Hard disk	The optional Removable HDD Kit enables administrators to physically remove the device's internal hard disk so it can be kept in a secure place after working hours. The drive can be easily reinstalled for use during normal working hours.
Secure boot	Secure Boot is a security standard to make sure that the device boots use only software that is trusted. When the printer starts, the controller software checks the signature of each boot software.
Data encryption	The hard disk encryption of the POWERsync controller encrypts all files present on the entire drive (including the operating system and all data; used space encryption). The encryption mechanism is based on a Trusted Platform Module (TPM) and Microsoft BitLocker mechanism which is compliant to FIPS 140-2 certification. The AES 256 encryption method is used.
HDD destruction at the end of the contract	The internal hard disk drive of the POWERsync controller can be removed and physically destroyed to ensure that no confidential data is stored in the printer.

AUTORISATION

Control panel access lock	With the access management function, the ClearConnect user control panel can only be accessed after unlocking via domain credentials or smartcard.
Secure printing via domain credentials (active directory)	The 'confidential' print jobs sent by the job owner are not printed until the job owner authenticates on the system user panel with the correct user credentials and releases them for printing.
Secure printing via smartcard (excl. Reader)	The 'confidential' print jobs sent by the job owner are not printed until the job owner authenticates on the system user panel by swiping and inserting the smart card and releases them for printing.
Print files only available in your Smart inbox	The print file will remain in your Smart Inbox until it is activated from the ClearConnect user panel or WebTools Express when 'direct print' is disabled. This function prevents the print from being taken by unauthorised users.
Scan to your personal home folder	The Scan to Home Folder function is available with the username and password authentication method. After entering authentication on the printer panel, the user can scan a file to his home directory on the network as configured for his own account on MS Windows Active directory.
Print from your personal home folder	The print from Home Folder function is available with the username and password authentication method. After entering authentication on the printer panel, the user can print from his home directory on the network as configured for his own account on MS Windows Active directory.
Disable ports and interface	To secure the POWERsync controller from unauthorised access, all unused ports and network interfaces are disabled.
Third party software such as uniFLOW	The PlotWave and ColorWave printing systems with a ClearConnect user interface can be integrated in uniFLOW environments. This gives users additional functionalities which help to control and reduce printing and copying costs, increase document security and improve employee productivity.

HACK PREVENTION

Disabling unused protocols	Network administrators are provided with the ability to configure the specific protocols that are accessible. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked.
SNMP V3	The secure version of SNMP which provides authentication and integrity between the Network Management Station (NMS) and the managed printers.
IEEE 802.1X device authentication	Port-based authentication mechanism (according to IEEE802.1X standard) is provided to allow a device to be authenticated by a central authority to communicate on the network with other devices.
McAfee antivirus (optional)	Optional possibility to install McAfee antivirus software on the POWERsync controller as an additional measure to protect against virus infections.
McAfee Whitelisting Application control (optional)	Optional security feature, activated via a license. When activated and enabled, it creates a detailed list of all the files on the controller and prevents any unauthorised change, whether by malware, viruses or unauthorised users. It constantly checks the integrity of files against the list and blocks any unauthorised change.

SECURE NOW AND IN THE FUTURE

Windows 10 IoT Enterprise LTSC controller software	The POWERsync controller in the printer uses Windows 10 IoT Enterprise LTSC.
Support to 2029 or beyond	Microsoft guarantees the support of Windows 10 IoT Enterprise LTSC to 2029 or beyond. This means security updates will be provided within this time period.
Remote controller security updates	Via WebTools Express, the system administrator can remotely upload and install security updates.
On Remote Service	On Remote Service is a service developed by Canon to ensure the highest uptime for your Canon system. As a controller embedded application, Remote Service offers you support at a distance including remote diagnostics, remote meter reading and remote assistance. It ensures increased system availability, reduced administration, improved first-time service fixes, quicker response times and above all, peace of mind.

Canon

Delighting You Always

Canon South & Southeast Asia Regional Headquarters
CANON SINGAPORE PTE. LTD.
1 Fusionopolis Place, #15-10 Galaxis, Singapore 138522
Tel : 65-6799-8888 | Fax : 65-6799-8882 | **https://asia.canon**

CANON BUSINESS PARTNER / DEALER'S STAMP

201001024928 (908810-T)
AUTOMATE S·Y·S·T·E·M
Sales & Services Sdn. Bhd.
603-5891 1628 6019-326 2916
careline.automate@gmail.com