SMARTshield

Integrated security for PlotWave and ColorWave printers

White paper

Canon

SMARTshield

Integrated security for PlotWave and ColorWave printers

White paper

July 2020

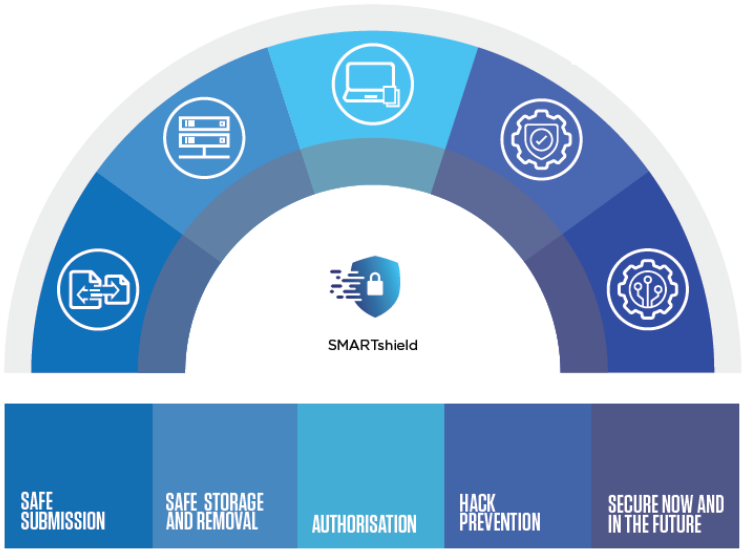
Table of Contents

Introduction

In the digital age, sharing information via printers and other networked devices is vital to working efficiently, but it also involves a certain level of risk. People, search engines and other devices may try to access your confidential business information. That means security is becoming an increasingly important discussion topic as organizations seek to protect their valuable assets within their large format working environment.

This Security White Paper is intended for IT administrators who would like to study the security features, system architecture and network impact of Canon Large Format printers. It explains the major security risks which may be encountered within large format printing environments and the measures we have taken to help you address them. The Security white paper is applicable for Océ PlotWave printers, Océ ColorWave printers, Canon PlotWave printers and Canon ColorWave printers.

The Canon security policy has been developed to ensure that our customers have a secure environment for printing, scanning and copying with their products. Our large format printing systems are designed to meet high security standards and reduce the risk of any security vulnerability. Our active involvement with customers, government agencies and security organizations enables us to identify and address new security threats in a timely manner as they arise. Thanks to these measures, you can be confident that your printing system contributes to a safe and secure IT environment.



SMARTshield – Integrated Printing Security Technology
Data security at every stage of the print workflow process:

- Safe submission
- Safe storage and removal
- Authorisation
- Hack prevention
- Secure now and in the future

The topics covered in this document relate to the following products:

- PlotWave® 300/340/345/350/360/365/450/500/550/750/900/3000/3500/5000/5500/7500
- ColorWave® 300/500/550/650/700/810/900/910/3500/3600/3700/3800/9000

SMARTshield is introduced with the PlotWave 3000/3500/5000/5500/7500 and ColorWave 3600/3800/9000. Many security features are also supported by the other products.
A summary of the security features per product is available at the end of this document. Some technical information in this document is subject to change: please consult the PlotWave and ColorWave Security Manual available on the Canon Production Printing download site (https://downloads.cpp.canon) for the latest details.

1. Security policy

We are committed to providing customers with systems that optimize their large format workflow while also providing a secure printing environment. To do this, we have established a comprehensive security policy and security organization that sets, implements and updates security features in our products.

Regulatory standards
The following regulatory standards are used to provide security guidelines for our products:

- STIG (Security Technical Implementation Guide)[1]
- Protection Profile for Hardcopy Devices: IPA (Information-technology Promotion Agency, Japan)[2], NIAP (National Information Assurance Partnership, USA)[3] and MFP (Multifunction Printer, Community)

Following the STIG (Security Technical Implementation Guide)
Since security vulnerabilities can have a negative impact on customer business, we have taken preventative measures to minimize potential threats by following the Multifunction device and network printers STIG. These rules provide a framework for our security program and aim to:

- Protect the global system integrity against attempts to modify the original controller, which can potentially jeopardize the productivity of the printing and/or scanning process.
- Mitigate the risk of the controller being used to penetrate the customer network.
- Prevent virus infection and protect against hacking actions.
- Protect the printer resources against illegal use.
- Ensure a high level of confidentiality for Canon and customer data.
- Increase the robustness of the global system (host application, controller, and engines).
- Ensure system availability by avoiding Denial of Service.

[1] https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=371
[2] https://www.ipa.go.jp/index-e.html
[3] https://www.niap-ccevs.org/

New products
The security policy is used to ensure that all newly developed products comply with the latest security requirements.

Vulnerability follow-up
Disclosed vulnerabilities related to our printing systems and their embedded controllers are monthly checked. Preventive or corrective measures or software patches are made available if required.

Participation in regulatory bodies
We work closely with customers, government agencies and security organizations to improve and develop security features for its products. We actively participate in the MFP Technical Community which is responsible for defining a Protection Profile (PP) to facilitate the efficient procurement of Commercial Off-The-Shelf (COTS) Hardcopy Devices (HCDs) using the Common Criteria (CC) methodology for information technology security evaluation. As a result, we are involved at the earliest stage in developing new technologies to meet new requirements described in the Protection Profile.

2. Safe Submission

Protect data and user credentials while sending files to your printer
from any device:

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

In a printing environment, protecting confidential data and proprietary information is essential. We have taken measures to protect user data from being altered or copied at all points in the workflow during network transfer. Some encryption mechanisms have been embedded to safeguard user data when it is being sent through the network to prevent any malicious hacker on the network from intercepting user data.

Access control (IP filtering)
Access control is a feature which uses IP filtering to limit the access to the printer. That means only equipment with specific IP addresses are allowed to communicate with the controller. This restricts the communications between the controller and other network equipment. You can configure up to 5 IP addresses.

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. When you configure Access Control, you can configure per IP address whether the communication from this host to the printer needs to be encrypted by IPsec. The encryption mechanism guarantees the confidentiality of the users' print and scan data on the network.

HTTPS
To protect the network traffic using the HTTP protocol from being intercepted or altered, the HTTPS protocol can be used instead of HTTP traffic with the controller. Moreover trusted certificates from a Certificate Authority can be embedded in the controller to prevent a man-in-the-middle attack, where a malicious party, which happens to be on the path to the controller, pretends to be the controller. The HTTPS protocol is always available.
The HTTPS protocol can be used to:

- Send encrypted print data to the printer controller via Publisher Express and Publisher Select.
- Save encrypted scan jobs from the printer controller (Scans Inbox).
- Securely manage the configuration of the system through Express WebTools / WebTools Express.[1]

[1] Depending on the printer model this is Express WebTools or WebTools Express.

IPv6 and IPv4 compatibility

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking 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 and can therefore address many more devices. You can choose to use IPv4 or IPv6.

Protecting password data

All the user passwords embedded in the system (Key Operator, System Administrator, Power User, external location passwords for Scan to File operations, pre-shared key for IPsec, Proxy authentication) are encrypted using strong cryptographic algorithms (AES128/AES256). No (encrypted) password can be transmitted outside the customer site without the authorization of the system administrator, for instance when he is performing a 'Save configuration' with Express WebTools / WebTools Express.

3. Safe Storage and Removal

Protect confidential data stored at the printer:

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

It is important to protect confidential data stored at the printer from being stolen or accidentally leaked from the company or department. By erasing data correctly, users can be sure their confidential files are unavailable to unauthorized colleagues.

Secure File Erase
You have multiple configuration options regarding storage of jobs on the printer:

- You can configure to remove jobs from the printer immediately after they are printed.
- You can configure the printer to automatically remove print, scan and copy jobs from the smart Inbox after a specified time.
- You can also decide to not keep a copy of print, copy or scan jobs in the smart inbox.

If you also enable E-shredding, then the files erase is secure.

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.

Three e-shredding algorithms may be set up on the controller by the System Administrator:

- DOD 5220.22-M: 3-pass overwriting algorithm (compliant with the US Department of Defense directive).
- Gutmann: 35-pass overwriting algorithm with random data.
- Custom: the user can set the number of passes, from 1 to 35.

Removable Hard Disk
Instead of fixed hard disks you can choose for removable hard disks. This optional Removable HDD Kit enables administrators to physically remove the device's internal hard disk after work hours and store it in a secure place.
The next working day he can take the hard disk from the secure place, install it again and start the printer.

Secure Boot
Secure boot is a security standard developed by members of the PC industry to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM).
When the device starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the device boots, and the firmware gives control to the operating system.

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). 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 128/AES 256 encryption method is used.
On some printer models it is an option, on some models it is a standard feature.
Also the implementation is model dependent. See the Security Manual for the model-specific information.

On some printer models it is an option and the disk encryption is performed during installation on the customer site. Two types of hard disk encryption can be chosen:

- Normal encryption which encrypts only the space used.
  This option speeds up the encryption at installation time (compared to full encryption) and is recommended for a new system integration.
- Full encryption which encrypts all the disk space used as well as empty space.
  This option is preferred for a system which is not new that may contain residual user data. This option is mandatory for some customers who must comply with strong security requirements (like the Department Of Defense).

On other models it is a standard feature and the disk is already encrypted in the factory. On these models there is only one type of disk encryption available: used space encryption and it always uses AES 256 encryption.

The hard disk encryption guarantees that customer data cannot be retrieved if the hard disk is stolen.

HDD destruction at the end of the contract
If the lease period ends, if the printer is exchanged for a newer or different model or if the printer is returned you can request to physically destruct the internal hard disk drive of the POWERsync controller to prevent leaving any usable data on the printer when it leaves your premises.

4. Authorisation

Restricts access to confidential files by unauthorised users:

- Control panel access lock
- Secure printing via domain credentials
- Secure printing via smart card
- Scan to your personal home folder
- Print from your personal home folder
- Print files only available in the Smart Inbox
- Disable ports and interfaces
- Third party software such as uniFLOW

Secure usage

With our printing systems, the user has no access to the software of the user interface and the Microsoft Windows embedded operating system. Only the functions for printing, copying and scanning are provided to the user.

The end user cannot do the following:

- Modify, install and run any other application (except a special secured option which exists for installing a third party application, such as installing an antivirus application).
- View, modify, delete or create any operating system setting.
- Browse the content of the disk.

Secure access

It is not possible to modify any operating system settings directly:

- The end user has no access to any direct operating system features.
- There is no possibility to directly update or upgrade the operating system.

Some operating system settings (like Network settings) can be changed within the password protected web application: Express WebTools/WebTools Express or with the ClearConnect touch screen interface.

User credentials for access

Four accounts have been designed with the permission to update configuration settings or to manage print, scan or copy jobs: Key Operator, System Administrator, Power User and Service. These accounts are specific to the controller application and are not Windows accounts. All four accounts are under customer control and are password protected (with salted Hash). Passwords are not readable.

Three of the accounts are available to customers:

- Key Operator - can manage jobs and change some printing and scanning settings without the authority to change network or system settings, such as Print/Copy and Scan preferences or Page Description Language (HPGL2, PDF, etc.).
- System Administrator - can manage the configuration settings, such as:
    - Connectivity settings
    - Security settings
    - External location settings

  Since this account has high access privileges it should be held confidential and only be accessible to selected individuals.
- Power User - has the rights of both the Key operator and the System Administrator.

The Service role is used exclusively by the service technician/dealer. With the latest controller releases, sensitive configurations/operations under the Service role are controlled by the System Administrator authorization.

User access (LDAP)
Instead of the local accounts for Key Operator, System Administrator, Power User and Service, the IT manager can also define which user, member of a domain (based on LDAP), can logon to the system via the device web interface or on the Local User interface with such a role.

Control panel access lock
If the printer supports access management, you can enable user authentication. If enabled, the ClearConnect user control panel will be locked and nobody can print, scan or copy. The user needs to unlock the printer with his/her user credentials. The user has to push the unlock button on the control panel and provide his or her credentials. This can be done by entering them or by smart card if the printer is equipped with a smart card reader.

Secure printing via domain credentials / secure printing via smart card
When user authentication is enabled

- The "sensitive" print jobs sent by the job owner are not printed until the job owner authenticates on the ClearConnect user control panel and releases them for printing.
- The print jobs are stored in the printer: only the job owner can access them.
- Copying and scanning operations are accessible only after the user authenticates on the ClearConnect user control panel.

Two different methods can be used for user authentication

- *User name & password*
  User name & password required on the ClearConnect user control panel.
- *A smart card*
    - *Smart card (PKI card MS Active Directory Certificates Services compatible)*
      A valid smart card must be inserted into the smart card reader (plugged into the USB outlet on the printer).
    - *Contactless card (PKI card MS Active Directory Certificates Services compatible)*
      A valid card without contact must be passed over a contactless card reader (plugged into the USB outlet).

Both methods require a Microsoft Active Directory environment.

Scan to your personal home folder / Print from your personal home folder
If user authentication is enabled and the method "user name and password" is selected, then the home folder comes available as one of the external locations. Next users can scan to or print form their home folder. Note that this home folder has to be enabled for the user's account in Microsoft Windows Active Directory.
Access to the home folder is performed through the LDAP protocol with the authentication performed through the Kerberos protocol. The data transfer (scan to / print from) is performed through the SMB protocol.
In case of Scan to home folder, it means only the respective user can retrieve his/her scans after he/she has authenticated on his/her own account on any workstation.

Print files only available in the Smart Inbox
You can disable direct printing on the printer. With Express WebTools / WebTools Express you specify that jobs can only be sent to the smart inbox. Now, drivers and submitters cannot print straight to the queue anymore. Every job goes to a smart inbox. Next the user has to activate the job via the ClearConnect user control panel or Express WebTools/WebTools Express.
This function prevents the print is taken by accident by other office workers.

Disable ports and interfaces
To secure the POWERsync controller from unauthorized 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 control panel can be integrated in uniFLOW environments of the customer. This gives users additional functionalities and help them to control and reduce printing and copying costs, increase document security and improve employee productivity. For more information, read https://www.uniflow.global/en/home/supported-devices/index.html.

5. Hack Prevention

Keep hackers out:

- Disabling unused protocols
- SNMPv3
- IEEE 802.1X device authentication
- (McAfee) antivirus
- McAfee Application control

One of the greatest security challenges for any business is keeping hackers out. With so much valuable data being printed, it's essential to prevent unwanted access to the printer and printer data.
And you want to be sure that your printer can't be hijacked and used against your network.

Controller security hardening
As new technologies and features become available, we are seeing new security threats to the network via the printing environment. To strengthen the security of the controllers, we are continuously hardening our software design policy. Some examples:

- Assessing all threats from security scanner reports. We evaluate them according to the actual level of threat to your printer/network and identify the false positive threats.
- USB hardening to prevent unauthorized USB usage and deny booting from USB.
- Prohibiting the system from being controlled with a keyboard/mouse including a virtual keyboard on the ClearConnect user control panel.
- Hardening web access with WebTools Express, for example disabling weak ciphers.
- Validation of input/output network traffic (e.g. for eliminating Cross site/Cross frame scripting, path traversal attacks and command injection).
- McAfee Application Control as an option on recent printers.

Print Files
The controller has been designed so that it will not execute or print any print files (or parts of print files) that are not recognized as a valid print file by the internal Page Description Languages (PDL) interpreter. This greatly reduces the chances of a corrupted file from infecting or damaging the actual controller. The PDLs supported are: HP-GL, HP-GL/2, CALS, TIFF, NIRS, CALCOMP, C4, JPEG, DWF (depending on the printer model), PostScript and PDF. PDF and PostScript are supported via the optional Adobe® PS3/PDF interpreter.

USB removable media
Preventative measures have been taken to provide a secure environment even when using USB removable media. It is not possible to boot from the USB key (except on a blank hard disk in cases where the hard disk is being replaced). It is not possible for the end user to browse to or execute any program present on a USB key.

Disabling unused protocols
To reduce the likelihood of an attack, only network protocols for printing and scanning have been implemented. All other protocols have been completely disabled. It is also possible for the end user to completely disable some protocols that are not used.
For a detailed specification of network protocols and services, please consult the PlotWave and ColorWave security manual via the Manuals section on https://downloads.cpp.canon (choose a printer and next select the Manuals tab and a language).

SNMP v3
The secure version of SNMP which provides authentication and integrity between the Network Management Station (NMS) and the managed printers.

TLSv1.2/Strong cipher
In high security environments, some old TLS protocol versions and some cipher suites may be prohibited, so it is possible to disable them while keeping the most secure one: TLSv1.2/strong cipher. Note that it is always possible to enable the old one only for compatibility with old browsers or specific web client applications in low security environments.

Device authentication (IEEE802.1X)
To provide a port-based authentication mechanism (according to IEEE802.1X standard) allowing a device to be authenticated by a central authority in order to communicate on the network with the other devices.

(McAfee) antivirus (optional)
We do not promote the installation of antivirus software on any controller since:
- We have taken significant preventive security measures to greatly reduce possible security threats, which should be sufficient in most customer environments.
- Antivirus software cannot be installed by the customer since there is no access to the normal Windows desktop and there are no privileges to install any software.
- The Windows operating system has been tailored with limited running components/services, and some of them may be required to run the antivirus installation program.

However, we understand that antivirus software may be requested by some customers. IT policy may dictate that particular antivirus software must be installed on all devices with a well-known operating system. To accommodate these situations, we have tested and approved two antivirus packages:
- Symantec Endpoint Protection
- McAfee VirusScan Enterprise Edition with ePolicy Orchestrator

A (Canon) Service Technician is needed to install these antivirus packages. The complete procedure to install these antivirus software packages is described in the Antivirus Installation Guideline. Please consult your Canon local representative for more information.

Important note: With antivirus software, there may be a situation in which the controller is reported as being infected when it is not actually infected. Antivirus software installed on the controller may intercept a virus infection hidden in a print file submitted to the controller. However, the controller never executes the malicious code. Therefore, the report to the Central Antivirus Server that the controller has been infected is incorrect.

McAfee Application Control (optional)

Some printers have the option McAfee Application Control. This feature is also known as white listing or McAfee Embedded Control.

Unlike a virus scanner, which can create a security risk if you do not keep it constantly updated with the latest virus definitions, McAfee Application Control creates a detailed map – a 'fingerprint' – of all the files on the printer and prevents any unauthorized changes, whether by malware, viruses or unauthorized users. It is constantly checking the integrity of the files against the fingerprint, and will block and report any tampering or unauthorized change.

If printer software needs to be upgraded, then the fingerprint will be updated as well. Installing 3rd party software like uniFLOW is to be done differently if this feature is enabled. After such an installation, the fingerprint is also updated.

6. Secure now and in the future

Keep your information secure: today and in the future:

- Windows controller software
- Remote controller security updates
- On Remote Service

Microsoft® Windows® embedded OS

The PlotWave and ColorWave controllers use an up-to-date Microsoft Windows embedded operating system (OS) or the latest Windows 10 IoT Enterprise LTSC which provides a very secure environment
for printing, copying and scanning with advanced lockdown capabilities. To further improve security and reduce vulnerability, we have:

- Disabled the most highly vulnerable modules on the Microsoft Windows embedded operating system.
- Either not installed or completely disabled all the components/features/services not used.
- Used a Windows account with reduced privileges for the controller programs.
- Configured the Windows firewall for minimal open ports for incoming and outgoing traffic connections.
- Used ACLs on system files to reinforce system security and integrity.
- Followed the Windows security reinforcement, including virtual account and keyboard filtering.

In addition to new features, we provide regular software releases with the latest security updates. We also embed the latest OS service pack in every new release of the controller, ensuring the highest level of security for customers.

Web access

Access to the controller is available remotely through the web application "Express WebTools"/"WebTools Express", which is based on a third party web server that generates pages on the fly with strong file restriction access and no link with the operating system.

Remote controller security updates

We check for Microsoft reports on operating system vulnerabilities and whether these vulnerabilities affect the PlotWave and ColorWave controllers monthly. Whenever vulnerability is reported, we update the Security Web page (https://downloads.cpp.canon) for each product.
If the controller is vulnerable, we follow a set procedure to provide a security update as soon as possible. Depending on the product, security updates are either patches developed by Canon Production Printing or genuine Microsoft security updates (.msu)

validated by us.
Because of this thorough testing, there is a delivery delay between genuine operating system security update availability and our security update availability.

Our security update procedure is a procedure for customers to use. The patch developed by us (applicable through our web application Express WebTools) is applied only if it is recognized as a genuine patch. This patch procedure has been designed to prevent someone from corrupting the controller. It is not possible to modify or corrupt the patch, and if this is attempted, the patch will be discarded.
The same procedure is used to apply a Microsoft security update (.msu).

Servicing the printer
Service employees use special procedures/features to configure, diagnose and troubleshoot the printer. With the latest generation of controllers, sensitive service operations are controlled by the System Administrator.

For service operations and systems requiring a service laptop:
- The connection between the laptop of the Service technician and the controller is made through a dedicated Ethernet connection.
- Service uses a dedicated account.

Canon Production Printing has a Security Policy which guarantees that the laptop of the Service Technician is always secured, updated with the latest Microsoft Security updates, with the latest antivirus signatures and protected by a firewall.

On Remote Service (ORS)
On Remote Service is a service developed by Canon Production Printing to ensure the highest uptime for your system. As a controller embedded application, ORS offers you support at a distance including remote diagnostics, remote meter reading and remote software uploading. The result is increased system availability, reduced administration, improved first-time service fixes, quicker response times and above all, peace of mind.

ORS has been designed to adhere to a high security standard therefore minimizing the risk of any security vulnerability. We have incorporated several security measures, control and user interaction aspects in the development of the ORS functionality:
- The customer is in control as he determines when and if Canon is allowed to connect remotely to the target device.
- ORS only retrieves printer device information and no information about customer documents.
- It is possible for a customer using ORS to see a history of the information that has been sent to Canon.
- ORS uses Industry Standard HTTPS connection methods for all communication between the device and our back office.

Data traffic between the customer site and Canon (from the PlotWave/ColorWave printer to the Canon Production Printing back office) is mainly outbound, except when a Remote Assistance session is ongoing. In the latter case the customer is always in control and can initiate or turn-off the remote session at their own discretion.

Download the ORS White Paper
This White Paper is intended for IT administrators who would like to study the security features, system architecture and network impact of ORS. It provides the detailed information about the following topics:

- Communication method(s) used by ORS in your network environment.
- Communication method(s) used by ORS for data transfer between print devices and the Canon Production Printing back office.
- Security prerequisite for installing and using ORS.
- Canon Production Printing Data Security Policy.

Download the ORS white paper via the Manuals section for a printer on https://downloads.cpp.canon (choose a printer and next select the Manuals tab and a language).

The printer architecture
A PlotWave or ColorWave printing system is composed of:
- A printer
- A controller
- A scanner (optional)
- Finishing equipment (optional)

The controller is the heart of printing system, driving the printing, copying and scanning processes. It has been developed and structured to ensure that the customer printing and working environment remains secure. The controller has been tailored to offer the best performance, productivity, reliability as well as the best serviceability. As such, it has been designed as a closed system.
- It is installed and supported by authorized users in the Canon Service & Support organization and at our dealers.
- A user can only access the features for printing, copying and scanning.

Security log
All the changes in the security section of the system are logged in a file which can be downloaded at any moment by the System Administrator (Audit Log feature). This allows the System Administrator to track all changes made to the settings.

Security Manual
The PlotWave and ColorWave Security Manual provides customers with detailed information about security measures implemented in printer, such as:
- Details of security features for each product
- Network ports used for external firewalls
- Tips, tricks and FAQs

This Security Manual is periodically updated to reflect the latest security enhancements in current and new products. It is available on the Canon Production Printing website (https://downloads.cpp.canon) on the Manuals section of each product page.

Appendix

Overview of security features per product
This section contains the security features for all PlotWave and ColorWave printers. For further details, please consult the PlotWave and ColorWave Security Manual.

PlotWave printers

	PW300 >= 1.5 PW350 >= 1.5 CW300 >= 1.5	PW750 PW900 R2	PW340 PW360 PW500	PW345 PW365 PW450 PW550	PW3000 PW3500 PW5000 PW5500 PW7500
Operating system	Microsoft Windows Embedded Standard 2009	Microsoft Windows Embedded Standard 7 SP1	Microsoft Windows Embedded Standard 7 SP1	Microsoft Windows Embedded Standard 8 64 bits	Microsoft Windows 10 IoT Enterprise LTSC 2019
Integrated Firewall	Yes	Yes	Yes	Yes	Yes
MS security flaws follow-up / Security patches (please check the security web page on https://downloads.cpp.canon).	Canon Production Printing released patches	Canon Production Printing released patches	Canon Production Printing released patches	Canon Production Printing released patches	Standard Microsoft Security update (.MSU) approved by Canon Production Printing
Network protocols protection	3 Security Levels	4 Security levels	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol
User authentication for Print/Scan	No	No	No	Yes, by: - User name and password - Smart card - Contactless card (R1.1 and higher)	Yes, by: - User name and password - Smart card - Contactless card
Device authentication (IEEE802.1X)	No	No	No	Yes (R1.2 and higher)	Yes
Express WebTools / User panel LDAP authentication	No	No	No	Yes (R1.2 and higher)	Yes
Scan to / print from Home directory (MS Active Directory)	No	No	No	Yes (Through Local User Authentication on Printer panel with Username/password)	Yes (Through Local User Authentication on Printer panel with Username/password)
Antivirus	Compatible with: - Symantec EPP 12.1 - McAfee VirusScan Enterprise Edition 8.8i	Compatible with: - Symantec EPP 12.1 - McAfee VirusScan Enterprise Edition 8.8i	Compatible with: - Symantec EPP 12.1 - McAfee VirusScan Enterprise Edition 8.8i	Compatible with : - Symantec EPP 14 for R1.1 and higher - Symantec EPP 12.1 for other releases - McAfee VirusScan Enterprise Edition 8.8i	Antivirus installation is supported.
IPV6	Yes (IPV6 and IPV4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)
SMB authentication	NTLMV1	NTLMV2	NTLMV2	NTLMV2	NTLMV2

	PW300 >= 1.5 PW350 >= 1.5 CW300 >= 1.5	PW750 PW900 R2	PW340 PW360 PW500	PW345 PW365 PW450 PW550	PW3000 PW3500 PW5000 PW5500 PW7500
SMB version for Scan To File	up to SMB1	up to SMB2.1	Up to SMB2.1	Up to SMB2.1	Up to SMB3.1.1
Data overwrite	E-shredding	E-shredding	E-shredding	E-shredding	E-shredding
Data encryption on the network	- IPsec	- IPsec - HTTPS (for administration with Express WebTools and for job submission through Publisher Express)	- IPsec - HTTPS (for administration with Express WebTools and for job submission through Publisher Express)	- IPsec - HTTPS (for administration with Express WebTools and for job submission through Publisher Express) - TLSv1.2 restriction possible.	- IPsec - HTTPS (for administration with WebTools and for job submission through Publisher Express and Publisher Select) - TLSv1.2 restriction possible.
SNMPv3	No	No	No	Yes (R1.2 and higher)	Yes
Hard disk encryption	No	No	No	Yes (Option) (TPM module required): 2 modes: - Normal - Full encryption - Encryption mode AES128 for R1.1 and lower - Encryption mode AES256 for R1.2 and higher	Yes (Standard): 1 mode: - Used space encryption - Encryption mode AES256
Access control (IP filtering)	No	No	Yes	Yes	Yes
Security logging	No	No	Auditing of security related events	Auditing of security related events	Auditing of security related events
Service operation restriction	No	No	No	Yes (with System Admin authorization)	Yes (with System Admin authorization)
Publisher Express access	Access by everyone	Access restriction possible	Access restriction possible	Access restriction possible	Access restriction possible
Removable Hard drive (option)	Yes	No	Yes	Yes	Yes
Secure Boot	No	No	No	No	Yes
McAfee Application Control	No	No	No	No	Yes (option)

ColorWave Printers

	CW550 CW600 CW650	CW500 CW700	CW3500 CW3700	CW3600 CW3800	CW810 CW900 CW910	CW9000
Operating system	Microsoft Windows Embedded Standard 7 SP1 for CW550/650 R3 Linux for CW550, CW600(PP) and CW650 R2 Linux and WES 2009 for CW550/650 R2 multifunctional (with scanner)	Microsoft Windows Embedded Standard 8 64 bits	Microsoft Windows 10 IoT Enterprise LTSB 2016	Microsoft Windows 10 IoT Enterprise LTSC 2019	Microsoft Windows Embedded Standard 8 64 bits	Microsoft Windows 10 IoT Enterprise LTSB 2016
Integrated Firewall	Yes	Yes	Yes	Yes	Yes	Yes
MS security flaws follow-up / Security patches (please check the security web page on https://downloads.cpp.canon).	Canon Production Printing released patches	Canon Production Printing released patches	Standard Microsoft Security update (.MSU) approved by Canon Production Printing	Standard Microsoft Security update (.MSU) approved by Canon Production Printing	Canon Production Printing released patches	Standard Microsoft Security update (.MSU) approved by Canon Production Printing
Network protocols protection	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol	Yes. Protection configurable per protocol
User authentication for Print/Scan	No	Yes, by: - User name and password - Smart card - Contactless card (R4.2 and higher)	Yes, by: - User name and password - Smart card - Contactless card	Yes, by: - User name and password - Smart card - Contactless card	No	No
Device authentication (IEEE802.1X)	No	Yes (R4.2 and higher)	Yes	Yes	Yes for CW910/810 R1.5 and higher version	Yes (R2.1 and higher)
Express WebTools / User Panel LDAP authentication	No	Yes (R4.2 and higher)	Yes	Yes	No	Yes
Scan to/print from Home directory (MS Active Directory)	No	Yes (Through Local User Authentication on Printer panel) for R4.1 and higher	Yes (Through Local User Authentication on Printer panel with Username / password)	Yes (Through Local User Authentication on Printer panel with Username / password)	No	No
Antivirus	Only for CW550/650 R3. Compatible with: - Symantec EPP 12.1 - McAfee VirusScan Enterprise Edition 8.8i	Compatible with: - Symantec EPP 12.1 - McAfee VirusScan Enterprise Edition 8.8i	Compatible with: - Symantec EPP 14 - McAfee VirusScan Enterprise Edition 8.8i	Antivirus installation is supported.	Only for CW910/810 R1.5 and higher. Compatible with: - Symantec EPP 14 - McAfee VirusScan Enterprise Edition 8.8i	Only for R2.1 and higher. Compatible with: - Symantec EPP 14 - McAfee VirusScan Enterprise Edition 8.8i
IPV6	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes for CW910/810 R1.5 and higher	Yes (R2.1 and higher)
SMB authentication	NTLMV2 or NTLMV1 for: - CW550/650 R2.2.3 and higher - CW550/650 R3 NTLMV1 for all other releases	NTLMV2	NTLMV2	NTLMV2	NTLMV2	N.A.

	CW550 CW600 CW650	CW500 CW700	CW3500 CW3700	CW3600 CW3800	CW810 CW900 CW910	CW9000
SMB version for Scan To File	Up to SMB2.1 for CW550/650 R3 Up to SMB1 for CW650 and CW550 multifunctional (with scanner)	Up to SMB2.1	Up to SMB3.1.1	Up to SMB3.1.1	N.A.	N.A.
Data overwrite	E-shredding for : - CW600 1.5 (and higher) - CW650(PP) and CW550	E-shredding	E-shredding	E-shredding	No	E-shredding
Data encryption on the network	IPsec for: - CW550 R2.3.1 and higher - CW650 R2.3.1 (PP) and higher	- IPsec - HTTPS (for admin-istration with Express WebTools and for job submis- sion through Publisher Express) - TLSv1.2 restriction possible	- IPsec - HTTPS (for admin-istration with Express WebTools and for job submission through Publisher Express) - TLSv1.2 restriction possible	- IPsec - HTTPS (for admin-istration with WebTools Express and for job submission through Publisher Express and Publisher Select) - TLSv1.2 restriction possible	- IPsec for CW910/810 R1.5 and higher - HTTPS (for administration with Express WebTools and for job submission through Publisher Express)	- IPsec - HTTPS (for administration with Express WebTools and for job submission through Publisher Express) - TLSv1.2 restriction possible
SNMPv3	No	Yes for R4.3 and higher	Yes for R5.1 and higher	Yes	Yes for CW910/810 R1.5 and higher	Yes for R2.1 and higher
Hard disk encryption	No	Yes (option) for R 4.1 and higher: - Encryption mode AES128 for R 4.1 - Encryption mode AES256 for R4.2 and higher	Yes (option), 2 modes: - Full disk encryption - Normal encryption Encryption mode AES256	Yes (standard), 1 mode: - Used space encryption Encryption mode AES256	No	No
Access control (IP filtering)	Yes for: - CW550 R2.3.1 and higher - CW650 R2.3.1 (PP) and higher	Yes	Yes	Yes	No	Yes
Security logging	Only for CW650 R3	Auditing of security related events	Auditing of security related events	Auditing of security related events	Auditing of security related events	Auditing of security related events
Service operation restriction	No	Yes (with System Admin authorization) for R4.1 and higher	Yes (with System Admin authorization)	Yes (with System Admin authorization)	No	Yes (with System Admin authorization)
Publisher Express access	Access restriction possible	Access restriction possible	Access restriction possible	Access restriction possible	Access restriction possible	Access restriction possible
Removable Hard drive (option)	Yes (for CW550 R3/ CW650 R3)	Yes	Yes	Yes	No	No
Secure boot	No	No	No	Yes	No	No
McAfee Application Control	No	No	No	Yes (option)	No	No

List of product abbreviations

PW300	PlotWave 300
PW340	PlotWave 340
PW345	PlotWave 345
PW350	PlotWave 350
PW360	PlotWave 360
PW365	PlotWave 365
PW450	PlotWave 450
PW500	PlotWave 500
PW550	PlotWave 550
PW750	PlotWave 750
PW900	PlotWave 900
PW3000	PlotWave 3000
PW3500	PlotWave 3500
PW5000	PlotWave 5000
PW5500	PlotWave 5500
PW7500	PlotWave 7500

CW300	ColorWave 300
CW500	ColorWave 500
CW550	ColorWave 550
CW600	ColorWave 600
CW650	ColorWave 650
CW700	ColorWave 700
CW810	ColorWave 810
CW900	ColorWave 900
CW910	ColorWave 910
CW3500	ColorWave 3500
CW3600	ColorWave 3600
CW3700	ColorWave 3700
CW3800	ColorWave 3800
CW9000	ColorWave 9000