Canon
CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE

OPTIMIZING SECURITY

Security white paper

Help safeguard your printing environment

April 2019

SMART CHANGE STARTS HERE.

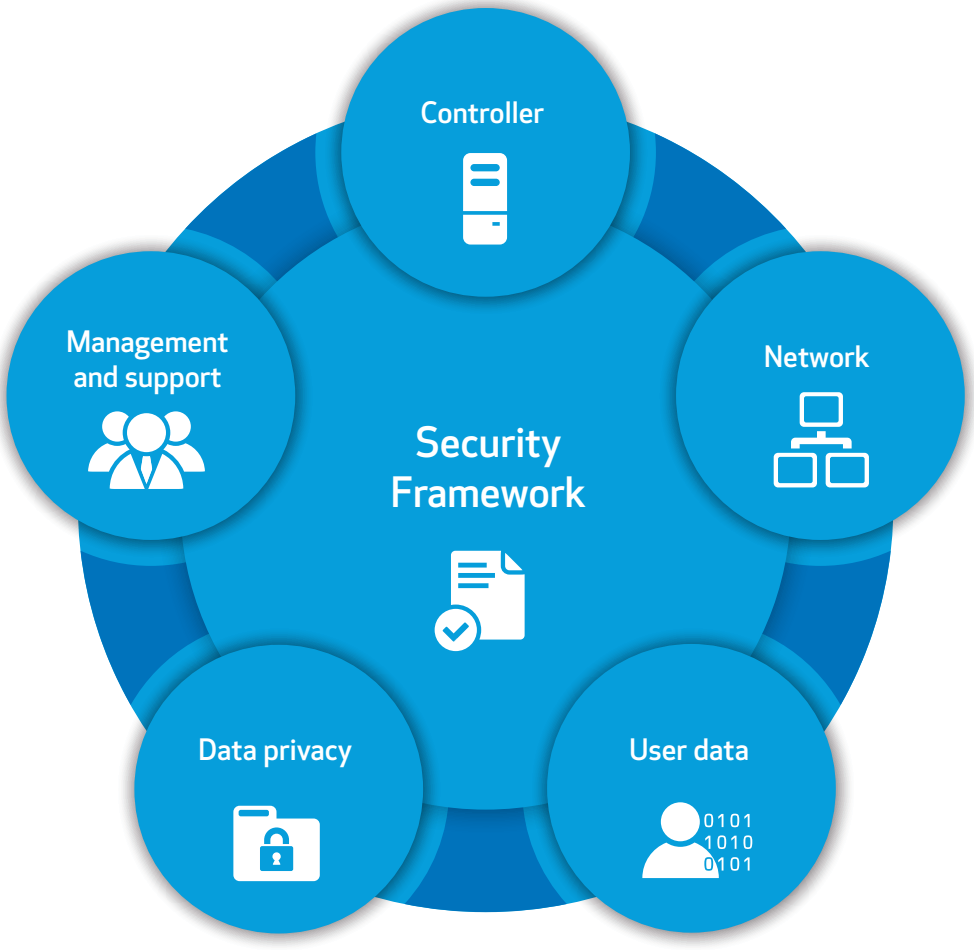
Table of Contents

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's Océ large format printing systems. It explains security risks that you may encounter within large format printing environments and the measures we have taken to help you address them.

Our active involvement with customers, government agencies, and security organizations enables us to identify and help address new security threats in a timely manner as they arise.



CANON'S OCÉ LARGE FORMAT SECURITY STRATEGY

- Secure controller
- Safeguard the network
- Safeguard user data
- Safeguard data privacy
- Safeguard management and support

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

- Océ PlotWave® 300/340/345/350/360/365/450/500/550/750/900
- Océ ColorWave® 300/500/550/650/700/810/900/910/3500/3700

A summary of 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 Océ Large Format Security Manual available on the Canon Solutions America corporate website (www.csa.canon.com) for the latest details.

1. Océ large format security framework

Canon is 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 framework. Within the Canon family, there is a group 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 vulnerability can have a negative impact on customer business, Canon has taken preventative measures to help reduce potential threats by following the multifunction device and network printers' STIG. These rules provide a framework for our security program and aim to help:

- 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 Océ Large Format system resources against illegal use
- Offer a high level of confidentiality for Canon and customer data
- Increase the robustness of the global system (host application, controller, engines)
- Provide system availability by avoiding denial of service

NEW PRODUCTS

Canon's Océ Research and Development group has implemented this security standard to ensure that all newly developed products are designed with the latest

security features. These standards are regularly updated based on changing market requirements.

VULNERABILITY FOLLOW-UP

Canon's Océ security organization checks the disclosed vulnerabilities related to our large format printing systems and their operating systems regularly and takes preventive/corrective (patch) measures when applicable.

PARTICIPATION IN REGULATORY BODIES

Canon works 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.

[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/

2. Secure controller

If your printer settings and controls are not secure, a person could intentionally or unintentionally change the settings on your printer, send print jobs somewhere else, or infiltrate your network. To help prevent this, controllers and customer networks must protect themselves from the risk of using the controller as a conduit for security threats. The Océ controllers provide security features to help ensure that only the authorized individuals can print, copy, and scan. This section explains how we have safeguarded the system architecture as well as the main operating systems to help prevent unauthorized access and changes to system settings. These measures have been put in place so that the system is used only for its intended purposes and to help prevent system access to unauthorized persons or devices.

- Architecture
- Operating System
- Security hardening
- Secure Usage
- Secure Access

OCÉ CONTROLLERS AND ARCHITECTURE

An Océ printing system is composed of an:

- Océ printer and/or scanner
- Océ controller

The Océ controller is the heart of Océ large format printing systems, driving the printing, copying, and scanning processes. It has been developed and structured so that the customer printing and working environment remains secure. The Océ controller has been tailored to offer outstanding performance, productivity, and reliability as well as serviceability. As such, it has been designed as a closed system.

- It is installed and supported by authorized users in the Canon Solutions America Service & Support organization and those of authorized Canon Solutions America Large Format Solutions dealers
- A user can only access the features for printing, copying, and scanning

OCÉ CONTROLLERS AND MICROSOFT WINDOWS-EMBEDDED OS

The Océ controllers use an up-to-date Microsoft Windows-embedded operating system (OS) or the latest Windows 10 IOT Enterprise LTSB to help provide a secure environment for printing, copying, and scanning with advanced lockdown capabilities. To further help 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 connections
- Used ACLs on system files to reinforce system security and integrity
- Followed the Windows security reinforcement, including virtual account and keyboard filtering

OCÉ CONTROLLERS SECURITY HARDENING

As new technologies and features become available, we see new security threats to the network via the printing environment. To help strengthen the security of the Océ controllers, we are continuously hardening our software design policy. The latest measures include:

- Assessing all threats from security scanner reports and evaluating them according to the actual level of threat to your printer/network and identify the false positive threats
- USB hardening to help 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 Océ ClearConnect software touch panel
- Hardening web access with Océ Express WebTools, 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)

SECURE USAGE

With Océ 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 that 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 (such as network settings) can be changed within the password-protected web application: Océ Express WebTools or with the Océ ClearConnect software touchscreen interface.

User credentials for access

Four accounts are designed with permissions 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, 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 select 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, the System Administrator authorization controls the sensitive configurations/operations.

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 or execute any program present on a USB key.

3. Safeguard the network

In a printing environment, the main security risks occur when connecting printers to the network. Canon has taken measures to reinforce network security to help prevent unauthorized access, hacking of print files, and infection of the controller.

- Web access
- Network protocols and services
- Access control (IP filtering)
- HTTPS
- TLSv1.2/Strong cipher
- Device authentication (IEEE802.1X)
- User access (LDAP)
- SNMPv3
- Print files
- Controller and antivirus software

WEB ACCESS

Access to the Océ controller is available remotely through the web application "Océ Express WebTools" 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.

NETWORK PROTOCOLS AND SERVICES

To help reduce the likelihood of an attack, only network protocols for printing and scanning were implemented. All other protocols have been disabled. It is also possible for the end user to disable some unused protocols.

For a detailed specification of network protocols and services, please consult the Océ Security Manual "Océ PlotWave/ColorWave Systems Security" via the Manuals section on http://csa.canon.com.

ACCESS CONTROL (IP FILTERING)

Access control is a feature that uses IP filtering to limit the access to the Océ large format system. 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.

HTTPS

To help protect the network traffic for Océ Express WebTools/Océ Publisher Express 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 server pretends to be the controller.

TLSV1.2/STRONG CIPHER

In a high-security environment, 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. It is always possible to enable the old one for compatibility with old browsers or specific web client applications in a low-security environment.

DEVICE AUTHENTICATION (IEEE802.1X)

This provides a port-based authentication mechanism (according to IEEE802.1X standard), allowing a device to be authenticated by a central authority to communicate on the network with the other devices.

USER ACCESS (LDAP)

Allows the IT manager to define which user, or member of a domain (based on LDAP), can log onto the system via the device web interface or on the Local User interface with either a Key Operator, System Administrator, or Power User role.

SNMPV3[4]

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

PRINT FILES

The Océ controller is designed to not execute or print any files (or parts of print files) that are not recognized as valid by the internal Page Description Languages (PDL) interpreter. This helps reduce 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, Adobe® PostScript,® and Adobe PDF. Adobe PDF and Adobe PostScript are supported through the optional Adobe PS3/PDF driver.

CONTROLLER AND ANTIVIRUS SOFTWARE

Canon does not promote the installation of antivirus software on any controller since:

- Canon has taken significant preventive security measures to help reduce possible security threats that 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 some customers may request antivirus software. IT policy may dictate the installation of particular antivirus software on all devices with a well-known operating system. To accommodate these situations, Canon has tested and approved two antivirus packages:

- Symantec AntiVirus Endpoint Protection
- McAfee® VirusScan® Enterprise Edition with ePolicy Orchestrator

An authorized Canon Solutions America Océ Large Format Service Technician is needed to install these antivirus packages. The complete procedure to install these antivirus software packages is described in the Océ Antivirus Installation Guideline. Please consult your local Canon Solutions America representative for more information.

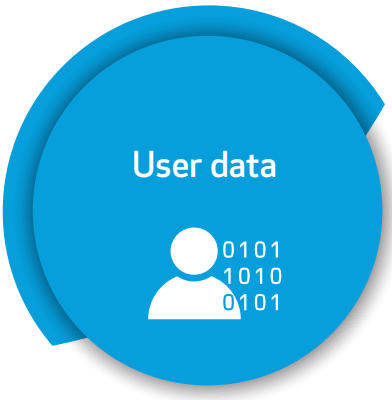
Important note:

With antivirus software, there may be a situation in which the Océ controller is reported as being infected when it is not actually infected. Antivirus software installed on the Océ 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 is infected may be incorrect.

[4] SNMPv3 is available for Océ ColorWave 3500/3700 Release 5.1 onwards, Océ ColorWave 500/700 Release 4.3 onwards, and Océ PlotWave 345/365/450/550 Release 1.2 onwards

4. Help safeguard user data

In a printing environment, protecting confidential data and proprietary information is essential. Canon has taken measures to help protect user data from being altered or copied throughout the workflow: during network transfer as well as on the device itself.



- Data on the network
- Data on the device

DATA ON THE NETWORK

Some encryption mechanisms have been embedded to help safeguard user data when it is being sent through the network to prevent any malicious hacker on the network from intercepting user data:

HTTPS

The HTTPS protocol can be used to:

- Send encrypted print data to the printer controller via Océ Publisher Express
- Save encrypted scan jobs from the printer controller (Scans Inbox)
- Securely manage the configuration of the system through Océ Express WebTools

Certificates are used to check the identity of the controller during the communication. The HTTPS protocol is always available.

IPSec

IPSec is a protocol that provides authentication, data confidentiality, and integrity in the network communication between the controller and other devices. You can connect up to five IPSec stations to the controller. The encryption mechanism provides the confidentiality of the users' print and scan data on the network.

DATA ON THE DEVICE

Once the user data transfers to the controller, Canon has embedded some mechanisms on the controller to help prevent malicious users from accessing this data.

E-shredding

The e-shredding feature is a security feature that allows the system to overwrite any user print/copy/scan data after it is deleted from the system. This feature helps prevent the recovery of any deleted user data (including file content and file attributes)—for instance, a stolen disk.

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

Hard disk encryption (option)

The hard disk encryption option of the Océ 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 that is compliant with FIPS 140-2 certification. The encryption method used is AES 128/AES 256.

The disk encryption is performed during installation on the customer site. Two types of hard disk encryption are available:

1. 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
2. Full encryption encrypts all used disk space used as well as empty space
    - Preferred for a system that is not new and may contain residual user data
    - This option is optimal for customers who must comply with strong security requirements (such as the Department of Defense)

The hard disk encryption option means that customer data cannot be retrieved if the hard disk is stolen — even if the TPM is stolen.

Protecting password data

All of 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). Encrypted passwords cannot transmit outside the customer site without the authorization of the system administrator — for instance, when they are performing a "save configuration" with Océ Express WebTools.

Letter of volatility

Each product has a letter of volatility that mentions the volatility of customer data stored in the various memory devices and engine. In other words, this letter outlines which data are stored on which memory when the printer is powered off (non-volatile) or powered on (volatile).

5. Help safeguard data privacy (user authentication)

The User Authentication option is designed to help protect sensitive print jobs and information from unauthorized access. Only the owner of the job can access the job.

- Secure printing/scanning
- Scan to/print from home directory
- uniFLOW*

SECURE PRINTING/SCANNING

When user authentication is enabled

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

Two different methods can be used for user authentication:

- Username and password: Username and password are required on the printer panel. This authentication method is mainly targeted for Windows-based environments (Microsoft Active Directory).
- Smart card (PKI card Microsoft 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 Microsoft Active Directory Certificates Services compatible): A valid card without contact must be passed over a contactless card reader (plugged into the USB outlet). The authentication method is mainly targeted to a Windows-based environment (Microsoft Active Directory).

SCAN TO/PRINT FROM HOME (OPTION)

The Scan to/Print from home option is available with the username and password authentication method. After entering authentication on the printer panel, the user can scan a file to (or print a file from) their home directory on the network, as configured for their own account on Microsoft Active Directory. They can access the home directory through LDAP protocol with an authentication performed through Kerberos protocol; data transfer (scan to/print from) occurs through SMB protocol. For the scan-to-home option, that means only the respective user can retrieve their scans after they have authenticated on their own account on any workstation.

uniFLOW

The latest Océ PlotWave and Océ ColorWave printing systems holding an Océ ClearConnect software user interface can integrate into the customer's uniFLOW environment. This gives users additional functionalities and helps 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.

* Requires a separate acquisition subscription of uniFLOW. Please speak with your Canon Solutions America representative for more details.

6. Help safeguard management and support

Despite the preventive security measures, Canon also takes measures to help protect the product after its release, including:

- Some vulnerabilities may be discovered after product installation. Canon has put a process in place to keep track of vulnerabilities and provide new releases with OS updates and patches after product installation.
- This helps ensure that the serviceability of the products is secure.

- Controller and OS updates
- Controller security patch updates
- Servicing
- Remote Service
- Security log
- Security Manual

OCÉ CONTROLLER/OS UPDATES

In addition to new features, Canon frequently provides software releases with the latest security updates. Canon also embeds the latest OS service pack in every new release of the Océ controller.

CONTROLLER SECURITY PATCH UPDATES (MICROSOFT AND OTHERS)

Canon checks for Microsoft reports on operating system vulnerabilities and whether these vulnerabilities affect the Océ controllers monthly. Canon updates the Océ Security web page http://downloads.oce.com for each product whenever a known vulnerability is reported.

If the Océ controller is vulnerable, we follow a set procedure to provide a software patch as soon as practicable. Patches developed by Canon are rigorously tested for the three latest releases on each Océ product. Because of this thorough testing, there may be a delivery delay between genuine operating system patch availability and Océ patch availability.

Note: The patches provided by Microsoft on the Microsoft website cannot be installed directly on the Océ controllers. Please use the appropriate Océ patches instead.

The Océ patch procedure is a procedure for customers to use. The patch (applicable through our web application Océ Express WebTools) is applied only if it is an Océ genuine patch. This patch procedure has been designed to help prevent someone from corrupting the Océ controller. It is not possible to modify or corrupt the patch, and if attempted, discard the patch.

SERVICING THE PRINTER SYSTEM

Authorized Canon Solutions America Océ Large Format Solutions service employees use special procedures/ features to configure, diagnose, and troubleshoot the Océ system. With the latest generation of Océ controllers, the System Administrator can control the sensitive service operations.

For service operations and systems requiring a service laptop:

- A dedicated Ethernet connection links the Océ Service Technician's laptop and the Océ controller
- Océ Service uses a dedicated account
- Canon has a Security Framework that provides that the Service Technician's laptop is secured, updated with the latest Microsoft Security updates and the latest antivirus signatures, and protected by a firewall

SECURITY LOG

All the changes in the security section of the system are logged in a file that the System Administrator can download at any moment (Audit Log feature). This allows the System Administrator to track all changes made to the settings.

OCÉ LARGE FORMAT SECURITY MANUAL

The Océ Large Format Security Manual provides customers with detailed information about security measures implemented in Océ large format printing systems, 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 Solutions America website on the Download/User Manual section of each product page under the heading "Océ Large Format Systems Security."

APPENDIX

Appendix: Overview of security features per product

This section contains the security features for all Océ large format printers. For further details, please consult the security manual.

PRODUCTS	PW300>=1.5, PW350>=1.5, AND CW300>=1.5	PW750 AND PW900 R2	PW340, PW360, AND PW500	CW810, CW900, AND CW910
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
Integrated Firewall	Yes	Yes	Yes	Yes
MS security flaws follow-up/Security patches	Océ-released patches	Océ-released patches	Océ-released patches	Océ-released patches
Network protocols protection	3 Océ security levels	4 Océ security levels	Yes: Protection configurable per protocol	Yes: Protection configurable per protocol
User authentication for Print/Scan	No	No	No	No
Device authentication (IEEE802.1X)	No	No	No	Yes (CW810/910 R1.5 and higher version) No (Other CW810/910 versions)
Océ Express WebTools/ User panel LDAP authentication	No	No	No	No
Scan to/Print from home directory (Microsoft Active Directory)	No	No	No	No
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	Only for CW810/910 R1.5 and higher version Compatible with: • Symantec EPP 14 • McAfee VirusScan Enterprise Edition 8.8i No (Other CW810/900/910 versions)
IPv6	Yes (IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (IPv6 only or IPv6 and IPv4 combination)	Yes (CW810/910 R1.5 and higher version) No (Other CW810/910 versions)
SMB authentication	NTLMV1	NTLMV2	NTLMV2	NTLMV2
SMB version for Scan to File	Up to SMB1	Up to SMB2.1	Up to SMB2.1	Up to SMB3.0.0

PRODUCTS	CW550, CW600, AND CW650	CW500 AND CW700	PW345, PW365, PW450, AND PW550	CW3500 AND CW3700
Operating System	• Microsoft Windows Embedded Standard 7 SP1 for CW350 R3 • Linux for CW550, CW600 (PP), and CW350 • Linux and WES 2009 for CW650 and CW550 multifunctional (with scanner)	Microsoft Windows Embedded Standard 8, 64 bits	Microsoft Windows Embedded Standard 8, 64 bits	Microsoft Windows 10 IoT Enterprise LTSB 2016
Integrated Firewall	Yes	Yes	Yes	Yes
MS security flaws follow-up/Security patches	Océ-released patches	Océ-released patches	Océ-released patches	Standard Microsoft Security Update (MSU) approved by Canon Océ (Please check Security web page on http://downloads.oce.com)
Network protocols protection	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: • Username/password • Smart card • Contactless card for CW500/700 4.2 and higher versions	Yes, by: • Username/password • Smart card • Contactless card (release 1.1 and higher)	Yes, by: • Username/password • Smart card • Contactless card
Device authentication (IEEE802.1X)	No	Yes for CW500/700 R1.2 and higher version No for other CW500/700 versions	Yes for PW345/365/450/550 R1.2 and higher version	No
Océ Express WebTools/ User panel LDAP authentication	No	Yes for CW500/700 R1.2 and higher version No for other CW500/700 versions	Yes for PW345/365/450/550 R1.2 and higher version	No
Scan to/Print from home directory (Microsoft Active Directory)	No	Yes (Through Local User Authentication on printer panel) for CW500/700 release 4.1 and higher No for CW500/CW700 release 4.0	Yes (Through Local User Authentication on printer panel with username/password)	Yes (Through Local User Authentication on printer panel with username/password)
Antivirus	Only for CW650 R3 compatible with: • Symantec EPP 12.1 • McAfee Virus Scan Enterprise Edition 8.8i	Compatible with: • Symantec EPP 12.1 • McAfee VirusScan Enterprise Edition 8.8i	Compatible with: • Symantec EPP 14 for PW345/365/450/550 1.1 and higher version • Symantec EPP 12.1 for other version • McAfee VirusScan Enterprise Edition 8.8i	Compatible with: • Symantec EPP 12.1 • 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)
SMB authentication	NTLMV2 or NTLMV1 for: • CW550 R2.2.3 and higher • CW650 R2.2.3 and higher • CW650 R3 • NTLMV1 for all other releases	NTLMV2	NTLMV2	NTLMV2
SMB version for Scan to File	Up to SMB2.1 for CW650 R.3 Up to SMB1 for CW650 and CW550 multifunctional (with scanner)	Up to SMB2.1	Up to SMB2.1	Up to SMB3.1.1

PRODUCTS	PW300>=1.5, PW350>=1.5, AND CW300>=1.5	PW750 AND PW900 R2	PW340, PW360, AND PW500	CW810, CW900, AND CW910
Data overwrite	E-shredding	E-shredding	E-shredding	No
Data encryption on the network	IPSec	• IPSec • HTTPS (for administration with Océ Express WebTools and for job submission through Océ Publisher Express)	• IPSec • HTTPS (for administration with Océ Express WebTools and for job submission through Océ Publisher Express)	• IPsec for CW810/910 R1.5 and higher version only • HTTPS (for administration with Océ Express WebTools and for job submission through Océ Publisher Express)
SNMPv3	No	No	No	Yes for CW810/910 R1.5 and higher version only
Hard disk encryption	No	No	No	No
Access control (IP filtering)	No	No	No	No
Security logging	No	No	Auditing of security-related events	Auditing of security-related events
Service operation restriction	No	No	No	No
Océ Publisher Express access	Access by everyone	Access restriction possible	Access restriction possible	Access restriction possible
Removable hard drive (option)	Yes	No	Yes	No
Letter of volatility	Yes	Yes	Yes	Yes

Appendix: List of Océ Product Abbreviations

OCÉ PLOTWAVE

PW300 ..... Océ PlotWave 300
PW340 ..... Océ PlotWave 340
PW345 ..... Océ PlotWave 345
PW350 ..... Océ PlotWave 350
PW360 ..... Océ PlotWave 360
PW365 ..... Océ PlotWave 365
PW450 ..... Océ PlotWave 450
PW500 ..... Océ PlotWave 500
PW550 ..... Océ PlotWave 550
PW750 ..... Océ PlotWave 750
PW900 ..... Océ PlotWave 900

PRODUCTS	CW550, CW600, AND CW650	CW500 AND CW700	PW345, PW365, PW450, AND PW550	CW810, CW900, AND CW910
Data overwrite	E-shredding for: • CW600 1.5 and higher version • CW650 (PP) and CW550	E-shredding	E-shredding	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 administration with Océ Express WebTools and for job submission through Océ Publisher Express) • TLSv1.2 restriction possible for CW500/700 R4.2 and higher version	• IPSec • HTTPS (for administration with Océ Express WebTools and for job submission through Océ Publisher Express) • TLSv1.2 restriction possible for PW345/365/450/550 R1.2 and higher version	• IPSec • HTTPS (for administration with Océ Express WebTools and for job submission through Océ Publisher Express) • TLSv1.2 restriction possible
SNMPv3	No	Yes for CW500/700 R4.3 and higher version only	Yes for PW345/365/450/550 R1.2 and higher version only	Yes for CW3500/3700 R5.1 and higher version only
Hard disk encryption	No	No for CW500/CW700 release 4.0 Yes for CW500/700 release 4.1 and higher: • Encryption mode AES128 for release 4.1 • Encryption mode AES256 for release 4.1 and higher	Yes (Option; TPM module required), 2 modes: • Normal • Full encryption • Encryption mode AES128 for release 1.1 and lower • Encryption mode AES256 for release 1.2 and higher	Yes, 2 modes: • Full disk encryption • Normal encryption • Encryption mode AES256
Access control (IP filtering)	Yes, for: • CW550 R2.3.1 and higher • CW650 R2.3.1 (PP) and higher	Yes	Yes	Yes
Security logging	Only for CW650 R3	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 release 4.1 and higher	Yes (with System Admin. authorization)	Yes (with System Admin. authorization)
Océ Publisher Express access	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
Letter of volatility	Yes	Yes	Yes	Yes

OCÉ COLORWAVE

CW300.....Océ ColorWave 300
CW500.....Océ ColorWave 500
CW550.....Océ ColorWave 550
CW600.....Océ ColorWave 600
CW650.....Océ ColorWave 650
CW700.....Océ ColorWave 700
CW810.....Océ ColorWave 810
CW900.....Océ ColorWave 900
CW910.....Océ ColorWave 910
CW3500.....Océ ColorWave 3500
CW3700.....Océ ColorWave 3700

WHY CANON SOLUTIONS AMERICA.

Canon Solutions America recommends forward-thinking strategies to help achieve the highest levels of information management efficiency for your unique business needs. Using superior technology and innovative services, we then design, implement, and track solutions that help improve information flow throughout your organization while considering the environment, helping to result in greater productivity and reduced costs.

There are many reasons why you should choose Canon Solutions America as your provider for document management solutions. Benefits include:

- A Canon U.S.A. Company
- Business Services
- Professional Services
- Global Monitoring Capabilities
- Certified Training and Support
- Flexible Finance Options
- Single-Source Solutions Provider
- Managed Document Services
- Nationwide Coverage
- Customized Industry Solutions
- Genuine Canon and Océ Parts and Supplies
- Diverse Range of Input-to-Output Technology

But that's not all. As a company that is dedicated to your needs, we support our solutions with highly skilled professionals and advanced diagnostic systems to maintain peak performance. And with ongoing consultation, we can further your document management capabilities to help ensure the highest level of satisfaction and productivity.

Canon

CANON SOLUTIONS AMERICA

Large Format Solutions

100 Park Blvd., Itasca, IL 60143

1-800-714-4427 | 1-630-250-6550

us.info@csa.canon.com **CSA.CANON.COM**

LFS-51373 DS 5/16/2019 CC1/PDF