Version 4.20
November 2025

White Paper: imageRUNNER ADVANCE DX imageFORCE & imagePRESS Lite Security

INTENT OF THIS DOCUMENT:

Canon recognizes the importance of information security and the challenges that your organization faces. This white paper provides information security information for Canon's imageRUNNER ADVANCE DX / imageFORCE / imagePRESS Lite systems (hereafter called Canon devices). It provides details on Canon devices security technology for networked and stand-alone environments, as well as an overview of Canon's device architecture, framework and product technologies as related to document and information security.

This White Paper is primarily intended for the administrative personnel of a customer charged with responsibility for the configuration and maintenance of Canon devices. The information in this document may be used to more clearly understand the many Canon devices-security-related configuration capabilities offered by Canon. The Canon devices offers a number of standard and optional capabilities. Ultimately, it is the customer's responsibility to select the method(s) that are most appropriate for securing their information.

Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its security features or recommendations will prevent security issues. Customers should perform their own due diligence and consult with their security expert to determine what security features to implement for their organization. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment.

Canon does not warrant use of the information contained within this document will prevent malicious attacks or prevent misuse of your Canon devices.

This document does not cover all models of the imageRUNNER ADVANCE DX and imagePRESS Lite product lines. For the scope of models please consult the Security Matrix. Products shown with optional accessories/equipment. The features reviewed in this white paper include both standard and optional solutions for Canon devices. For the latest security features supported by model please consult the Security Matrix. Specifications and availability subject to change without notice. https://partners.usa.canon.com/online/myportal/partners/home/security

Table of Contents

Section 1 — Introduction

1.1– Security Market Overview

In today's digital world, risks to networks and devices come in more forms and from more directions than ever before. From identity theft and intellectual property loss to infection by viruses and Trojan horses, IT administrators today find themselves playing an additional role of security officer in their efforts to protect information and assets from threats from the outside as well as within.

On a regular basis, potentially destructive threats emerge and undiscovered vulnerabilities are exposed, proving that you can never be too secure. IT administrators need a holistic security strategy that can be applied at every level of the organization — from servers, desktops and devices such as MFPs, to the networks that connect them all.

Also, increased governmental regulations add an additional layer of strict compliance standards that must be met. Legislation such as Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights Privacy Act (FERPA), Homeland Security Presidential Directive (HSPD)-12, California Consumer Privacy Act (CCPA), among others, all have various requirements that organizations need to take into account.*

**Note: Canon U.S.A. does not provide legal counsel or compliance consultancy, including without limitation, SOX, HIPAA, GLB, FERPA, HSPD, CCPA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.*

1.2– Imaging & Printing Security Overview

Any networked Multifunction Printer is potentially at risk of being attacked through the network. For this reason, MFPs require security measures just like PCs. Techniques of malicious adversaries evolve and it is required not only to take actions against existing attack methods but also to provide a multi-layered defense with multiple proactive protection methods. Furthermore, because an MFP is also a document handling device, in addition to IT device security measures, document-specific security measures such as implementing features are designed to help in organizations efforts to limit printout take-away, are also important.

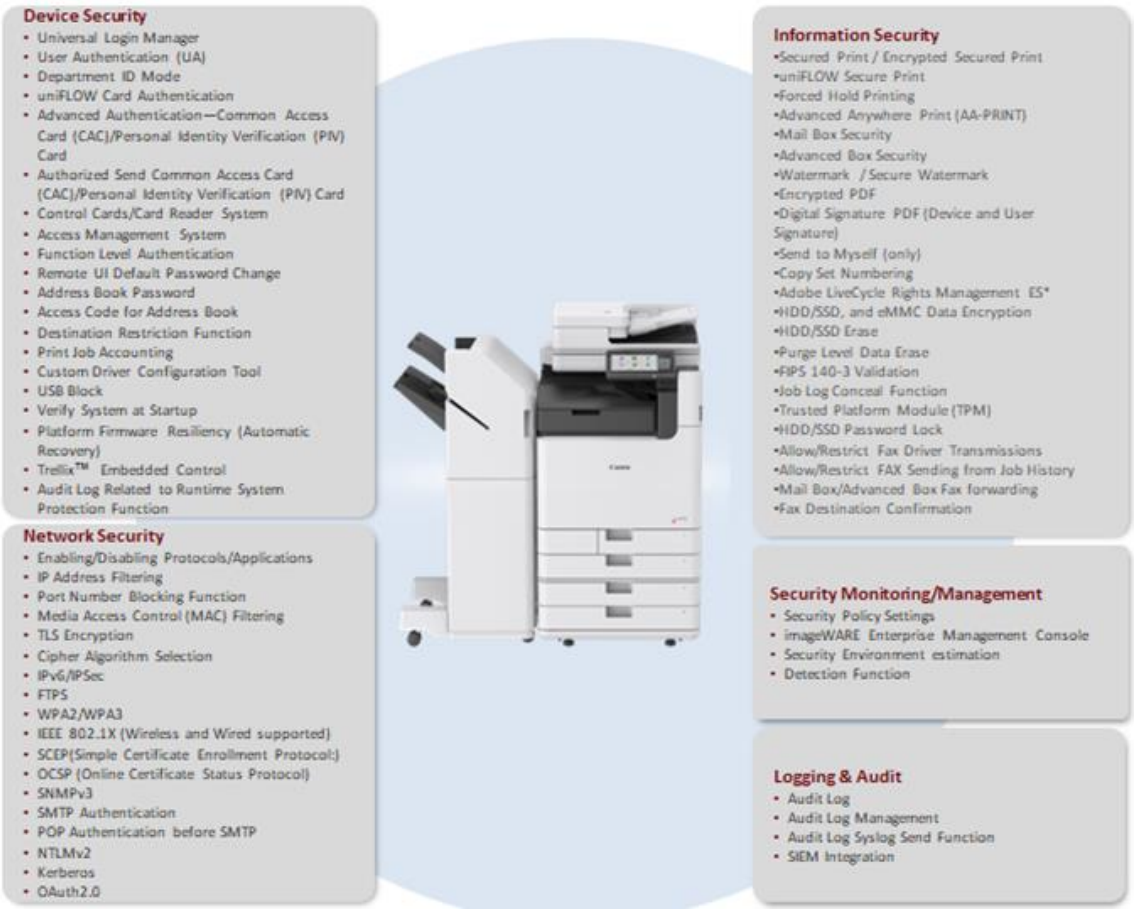
The Canon devices Security White Paper has been designed to provide detailed information on how Canon devices provide security features that organizations can implement. Canon devices are designed with features that can be used to help organizations in their efforts to protect not only the MFP (Multi-Function Printer) system itself, but also the customer assets associated with the MFP—such as information assets that enter and exit the MFP via the network, those stored within the device, and those printed out.

1.3– Key Security Concentration Areas

Canon devices categorize the numerous security features that are designed to help organizations in their efforts to protect both the MFP itself and associated information assets into the following five key areas:

- Device Security
- Information Security
- Network Security
- Security Monitoring / Management Tools
- Logging & Auditing

Canon dedicates a significant amount of time and resources to improve the security capabilities of Canon devices. Numerous capabilities are available for administrators to restrict access to the device's features and functions at a granular level, while maintaining high availability and productivity.



**Note: Functionality varies by model.*
See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if features are available for device capabilities. Please be sure to check back before purchasing, as specifications and availability are subject to change.

Section 2 — Device Security

This chapter provides an overview of the enhanced device security functions.

Canon devices are equipped with various security functions to help organizations in their efforts to prepare for the growing number of threats in the world. Specifically, they feature multiple authentication methods, access control to help manage device functions and internal data, and advanced measures designed to help limit malware intrusion and tampering.

2.1– Authentication

Canon devices offer multiple authentication options for administrators. These options allow authenticated users to access the device and its functions such as printing, copying, scanning, and sending. Authentication restricts access to Canon devices from unauthorized users and allows administrators to control color output usage and total print volume.

2.1.1 Device-Based Authentication:

Authentication using uniFLOW Online (Universal Login Manager Authentication)
Provides login functionality before operating the device using Universal Login Manager (ULM) offered by additional purchase of uniFLOW Online. Supports PIN, card authentication, and multi-factor authentication combining both. Also supports function-specific authentication, allowing access only to specific functions like copy or print.
** Note: Multi-factor authentication support varies by model.*

User Authentication (UA) *Functionality varies by model.
If available, User Authentication allows login before device operation using users registered on the device, Active Directory/LDAP servers, or Entra ID (formerly Azure Active Directory). This functionality also supports function-specific authentication.

Department ID Authentication *Functionality varies by model.
Built-in feature on some Canon devices that allows administrators to control access to the device. When enabled, users must enter a password before accessing the device. Department IDs can restrict access to functions like mailboxes, fax, print, and copy.

**Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.1.2 Card-Based Authentication:

uniFLOW Card Authentication
When combined with the optional uniFLOW solution, Canon devices are able to authenticate users through contactless cards, chip cards, magnetic cards and PIN codes. uniFLOW supports HID Prox, MIFARE, Legic, Hitag and Magnetic cards natively using its own reader, as well as others through custom integrations. Certain models of RF Ideas Card Readers can also be integrated to support authentication using radio-frequency identification (RFID) cards.
**Note: Cards and Card Readers must be purchased separately.*

Advanced Authentication: Common Access Card (CAC) / Personal Identity Verification (PIV)
Federal agencies—both civilian and military (DoD)—require enhanced user authentication and data security features to help in their efforts to comply with the requirements of the Homeland Security Presidential Directive 12 (HSPD-12). Employees must verify their identity and security classifications using secure and reliable forms of identification, such as Common Access Card (CAC) and Personal Identity Verification (PIV). And with networked multifunction printers (MFPs) being deployed on a greater scale in these locations, Canon developed Advanced Authentication CAC/PIV—an easy-to-use, two-factor embedded authentication solution to lock and unlock Canon devices. This serverless solution allows all

device functions to be standby until users insert their government-issued Common Access Card/Personal Identity Verification into the card reader and enter their PIN. Only those authenticated individuals are granted access to the device. This also supports FIPS 140-2 validated cryptography and integrates with AMS for device feature access control.

Authorized Send CAC/PIV

To fulfill the strict security requirements of government agencies as dictated by Homeland Security Presidential Directive-12 (HSPD-12), Canon devices support the use of Common Access Card (CAC) and/or Personal Identity Verification (PIV) card authentication for the embedded Authorized Send MEAP application. Authorized Send for CAC/PIV is a server-less application that is designed to help protect the Scan-to-Email, Scan-to-Network Folder and Scan-to-Network Fax functions, while allowing general use of walk-up operations like print and copy. This also integrates with AMS for granular access control of ASEND functionality.

Authorized Send for CAC/PIV supports two-factor authentication by prompting users to insert their card onto the device's card reader and requiring them to enter their PIN. ASEND for CAC/PIV supports the Online Certificate Status Protocol (OCSP) to check the revocation status of the user's card and then authenticates the user against the Public Key Infrastructure (PKI) and Active Directory. Once authenticated, users can access the document distribution features of Authorized Send.

Authorized Send for CAC/PIV supports enhanced e-mail security features such as non-repudiation, digital signing of e-mail, and encryption of e-mail and file attachments. The cryptographic engine used by Authorized Send for CAC/PIV has undergone the stringent testing and validation requirements of the FIPS 140-2 standard.

** Note: The signing of email and encryption of email are optional by default - the user must enable either or both ones during the operation.*

Control Card/Card Reader System Option

Canon devices offer support for an optional Control Card/Card Reader system for device access and to manage usage. The Control Card/Card Reader system option requires the use of intelligent cards that must be inserted in the system before granting access to functions, which automates the process of Department ID authentication. Cards must be purchased separately.

2.2– Access Control

Canon devices support access control to help organizations manage device settings and function usage. Canon offers solutions that can either lock the entire device or restrict only specific functions (e.g., Send-to-Email), while allowing access to others.

2.2.1 Access Management System (AMS): *Functionality varies by model.

The Access Management System, which is standard on some Canon devices, can be used to tightly control access to device functionality. Restrictions can be assigned to users and groups, to restrict entire functions or restrict specific features within a function. Access restrictions are managed in units called "roles". Roles contain information that determines which of the various functions of the device may be used or not. Roles can be set up based on individual user's job title or responsibilities or by group, enabling the administrator to create roles specific to certain departments or workgroups. This allows administrators to create roles tailored to specific departments or workgroups. System administrators can configure roles to meet various business needs, such as restricting specific functions. In addition to default roles with preset access restrictions, new custom roles can be registered. Guest users can also be defined and assigned roles.

Custom roles can restrict the following functions:
- Copy
- Scan and Send
- Fax
- Secure Print
- Access Stored Files
- Scan and Store
- Fax / I-Fax Inbox
- Hold
- Scanner

- Printer
- Tutorial
- Web Access
- Destination / Forwarding Settings
- Web Access Favorites
- MEAP Application

When the Access Management System (AMS) is enabled, users must log in using Universal Login Manager (ULM) or User Authentication (UA). AMS supports Active Directory authentication using UA, including Kerberos authentication. Once a user logs into the device with their username and password, based on the administrator pre-configured set roles, the device can determine which roles are assigned to that particular user. Restrictions are applied based on the assigned roles. If an entire function is restricted, it will appear grayed out to the user after authentication.

Function-Level Authentication: *Functionality varies by model.
Select Canon devices offer the ability to limit the use of specific functions by authorized users by requiring authentication to use sensitive functions with Function Level Authentication. Function Level Authentication is a part of Access Management System and works with ULM, UA, or SSO-H for authentication. It enables administrators to choose precisely which functions are permitted by walk-up and network users without entering credentials versus the ones that require a user to login. For example, administrators may choose to allow all users to make black-and-white copies while prompting users to login if they choose to output color or use the Scan and Send function.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.2.2 Password-Protected System Settings:

Canon devices come standard with password protection for system settings accessed via the control panel or Remote UI. System Administrators can set network information, system configuration, enable, and disable network and printing protocols among many other options**. The password-protected system settings is recommended to be enabled at the time of install by an administrator and choose a password since it controls critical device settings.**

Remote UI Default Password Change
Due to increasing global regulations on the security of network-connected electronic devices like printers and Wi-Fi routers, many laws now require devices to either have a unique password per unit or prompt users to change the default password before use. Canon complies with these requirements by disabling remote access until the default password is changed.

2.2.3 Scan and Send Security:

On devices that have Scan and Send enabled, certain information such as fax numbers and e-mail addresses may be considered confidential and sensitive. For these devices, enabling scan and send security feature will assist in the protection this information, offering additional security features that can be enabled to limit unauthorized access.

Address Book Password:
Administrative and individual passwords can be set for Address Book Management functions. A system administrator can define the specific Address Book data that can be viewed by users, effectively masking private details. This password may be set separately so individuals other than the System Manager can administer the Address Book.
By setting a password for an Address Book, the ability to Store, Edit, or Erase individual and group e-mail addresses in the Address Book is restricted. Therefore, only individuals with the correct password for an Address Book will be able to make modifications.
This is not the same functionality when password protecting an Address Book. Administrators who are looking to Import/Export an Address Book, can elect to set a password when exporting the File. That password is then required to Import the Address Book. The Address Book Import/Export function is available through the Remote UI utility.

Address Book Access Code: *Functionality varies by model.

On select Canon devices, End-users will also have the capacity to place an access number code on addresses in the Address Book. When registering an address, users can then enter an Access Number to restrict the display of that entry in the Address Book. This function limits the display and use of an address in the Address Book to those users who have the correct code. The Access Number can be turned on or off, depending on the level of security the end-user finds necessary. The system administrator can access all address books regardless of whether the Access Code is set or not by users.

Destination Restriction Function:

Data transmission to a new destination through the Scan and Send and Fax function can be restricted, prohibiting transmissions to locations other than the destinations registered or permitted by the System Manager. By restricting sending of faxes, e-mails, I-faxes, and files to new destinations using the procedure below, data can only be sent to previously registered destinations. As you can no longer enter or send to new destinations, setting this mode with an Address Book PIN provides an additional layer of security when sending. Sending is only allowed in the following cases when this mode is set:• If you specify a destination stored in the Address Book

- If you specify a destination obtained via an LDAP server
- If you specify a destination by pressing a one-touch button
- If you recall stored [Favorite Settings] including destinations
- If you select [Send to Myself]

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.2.4 Print Driver Security Functions:

Print Job Accounting *Functionality varies by model.

A standard feature on select Canon device's printer drivers, print job accounting requires users to enter an administrator-defined password prior to printing, thereby restricting device access to those who are authorized to print. Printing restrictions can be set using Department ID credentials, User Account Credentials, or through the Access Management System.

Custom Driver Configuration Tool

Administrators can create custom driver profiles for users to limit access to print features and specify default settings, this allows organizations to help protect the device against unauthorized use, enforce internal policies and better control output costs. Security conscious settings that can be defined and enforced include duplex output, Secure Print feature, B&W only on color devices, watermarks and custom print profiles, as well as hiding desired functions.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.2.5 USB Blocking *Functionality varies by model.

USB Block allows the System Administrator to help protect the Canon device against unauthorized access through the built-in USB interface. Access to the device's USB interface for desktop access and the device's host mode for other USB devices can each be permitted or disabled. While USB memory usage can be restricted, USB peripherals such as keyboards and card readers are still permitted. Canon devices only allow viewing and printing of non-executable files such as .pdf, .jpg, .tiff, and .png via USB. To activate this feature, ensure the function is turned on.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.2.6 Third-Party MEAP Applications and Development *Functionality varies by model.

Canon actively collaborates with major software vendors to develop custom MEAP (Multifunctional Embedded Application Platform) applications.
Access to the Software Development Kit for MEAP is tightly restricted and controlled through licensing. Once an application has been developed, it is thoroughly reviewed by Canon to ensure that it meets strict guidelines. Following the review, the application is digitally signed with a special encrypted signature to help protect the integrity of the application. If the application is modified , the signature code will not match and the application will not be permitted to run on the device. These safety measures are designed to make it virtually unable for an altered or rogue MEAP application to be executed on a Canon device.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.3– Security Measures Against Malware and Firmware/Application Tampering *Functionality varies by model.

Some Canon devices include security features designed to help limit malware and firmware tampering. During firmware updates, process execution, or MEAP application installation, any program lacking a Canon-issued digital signature cannot be installed or executed.
The following tamper detection features have been introduced:

- Verify System at Startup (off by default. Must be turned on)
- Platform Firmware Resilience (Automatic Recovery)
- Trellix™ Embedded Control (off by default. Must be turned on)

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if these features are available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

2.3.1 Verify System at Startup *Functionality varies by model.

Once enabled on a compatible Canon device, the Verify System at Startup function runs a process during startup to verify that tampering of boot code, OS, firmware and MEAP applications has not occurred. If tampering of one of these areas is detected, the system will not start. By using the hardware as the 'Root of Trust', this is designed to provide enhanced security against software tampering. Furthermore, standard cryptographic technologies (hash, digital signature) are used for verification.
To use this feature, administrators must change the default setting from OFF to ON. When this function is turned ON, warmup time is increased because the verification process is performed when the device is started. However, it does not affect the time to wake up from sleep mode or the restore time for quick startup, because the verification process is only performed at device startup.
If tampering of boot code/OS/firmware/MEAP applications is detected, the device boot process is halted, and an error code is displayed on the control panel. In order to recover from that state, it may be necessary to reinstall the firmware/MEAP application.

2.3.2 Platform Firmware Resilience (Automatic Recovery) *Functionality varies by model.

The Platform Firmware Resiliency is firmware automatic recovery function. On a compatible Canon deice, this feature will attempt to continue operation using the backup program without stopping the startup when an unauthorized program is detected by Verify System at Startup.
More specifically, when an unauthorized operation is detected in started program, it is overwritten with a program in the backup area. If both the normal startup program and the backup area program are illegal programs at the same time, startup will be stopped.

2.3.3 Trellix™ Embedded Control *Functionality varies by model.

Once enabled on a compatible Canon device, Trellix™ Embedded Control is designed to allow only known programs contained in the dynamic whitelist to be executed on the MFP. **To turn on Trellix™**

Embedded Control, it is necessary to turn on Verify System at Startup (Default OFF). The administrator will also need to set "Trellix™ Embedded Control" to ON (Default OFF). Other programs not listed in the whitelist are considered unauthorized and will not be permitted to execute. This is designed to help limit worms, viruses, spyware, and other malware from compromising the device. Trellix™ Embedded Control is designed to help

- Provides file integrity of Canon authorized firmware/applications against the whitelist to help limit tampering.
- Limit the execution of unknown software code (malware) not on the whitelist.
- Limit unauthorized rewriting of registered software modules.
- Detect tampering of the whitelist itself.
- Permits only authorized system processes to implement changes on device.

The firmware verification process begins when a whitelisted execution module is launched. If verification fails, execution is blocked and an error code (E614-xxxx) is displayed.
If an attempt is made to execute an unregistered software module, it is blocked and the event is logged. Attempts to rewrite or delete registered modules are also blocked and logged.
Whitelist verification occurs at software module startup. If tampering is detected, execution is blocked and an error code is displayed based on the location of the tampered module.
The whitelist is updated as needed when system firmware is updated or authorized MEAP applications are installed. To maintain consistency, the whitelist and its change history (transaction log) are also updated when software modules are updated.
Recordable activities related to Verify System at Startup and Trellix™ Embedded Control's runtime intrusion detection is logged in the device management log and can be reported in real-time to security administrators if an organization integrates a compatible Canon device with a compatible SIEM system. (Third party SIEM system required. Subject to third party SIEM system terms and conditions. Canon cannot ensure compatibility with all third party SIEM systems.)

Section 3 — Information Security

Canon devices are equipped with a variety of security features. From documents, faxes, and emails to data stored on internal hard disk drives and memory, Canon incorporates numerous security features organizations can implement as part of their efforts to protect information while using Canon devices.

3.1-Document Security

3.1.1 Secure Print feature

Secure Print / Encrypted Secure Print
Canon devices offer Secure Print and Encrypted Secure Print features.

Secure Print
This feature requires the user to enter a pre-specified password at the time of printing. The user sets a password in the printer driver interface and then enters the same password on the Canon device to initiate printing.

Encrypted Secure Print
Canon devices enhance security by encrypting print data before transmitting it to the Canon print device. This function uses AES 256-bit encryption.

System administrators can configure the print job restriction feature to allow only encrypted print jobs. Please refer to the Security Matrix for supported models.

uniFLOW Secure Print
Canon offers an additional purchase of uniFLOW solution that integrates with Canon devices. It provides encryption for both communication paths and print data, holds print jobs on the server until a security code is entered, and extends user authentication capabilities. This solution supports use cases such as printing company data at home using a system and communication channel that contains security features.

Forced Hold Printing * Functionality varies by model.
Some Canon devices can be configured to require hold printing. Please refer to the Security Matrix for supported products. This setting must be changed via the local device UI under the [Settings/Registration] screen. There is no need to modify the printer driver settings.
System administrators can configure how long held print jobs are retained. They can also choose whether to automatically delete the job after printing, retain it until it expires, or require manual deletion.

AA-Print (Advanced Anywhere Print) * Functionality varies by model.
Advanced Anywhere Print (AA-PRINT) is a serverless MEAP solution for some Canon devices that combines the productivity of a print-anywhere solution integrated with ULM. Users can print and release their jobs from any compatible Canon device connected to the network. AA-PRINT uses the Advanced Box (a Canon feature) as a server for storing print jobs and user data required for authentication.
AA-PRINT is ideal for small to medium-sized organizations seeking a simple and cost-effective way to implement a print security feature, help reduce maintenance costs and help maximize productivity—without the need for additional servers or associated maintenance overhead.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.1.2 Protection of Document Storage Areas

Mailbox Security * Functionality varies by model.

Some Canon devices include a user data storage area known as the "Mail Box" feature. This area is protected by a password. Please refer to the Security Matrix for models that support the Mail Box feature.

Advanced Box Security * Functionality varies by model.
Some Canon devices allow internal storage areas to be used as shared storage, a feature known as "Advanced Box." Please refer to the Security Matrix for supported models.
Advanced Box restricts stored files to printable formats such as TIFF, JPEG, and PDF. When shared as a network drive, it can also be scanned by antivirus software. Detailed settings for Advanced Box are configured by the administrator via the Remote UI interface.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.1.3 Other Document Security Features

Watermark / Secure Watermark
To help limit unauthorized copying or transmission of confidential information, Canon devices support the ability to embed user-defined text into the background of printed or copied documents. When a document is copied, a watermark becomes visible. The watermark feature can be applied to all print jobs by default or assigned by the user through the print driver. Users can also define custom or preset watermarks to appear at any location on the copied output.

Encrypted PDF * Functionality varies by model.
In Encrypted PDF mode on compatible Canon devices, security can be enhanced by encrypting PDF files sent to email addresses or file servers, setting passwords, and defining access permissions. If implemented by an organization, only users who enter the correct password can open, print, or modify the received PDF files.

Encrypted PDF mode is available only when the destination is an email address or file server. If the destination is a fax number, I-Fax address, or inbox, users cannot send the job as an encrypted PDF file. Canon devices use AES 256-bit encryption for PDF files.

Digitally Signed PDF (Device and User Signatures) *Functionality varies by model.
With the Scan and Send function, a digital signature can be added to PDF or XPS documents to help users verify their source and authenticity on compatible Canon devices. When a recipient opens a PDF or XPS file saved with a digital signature, they can view the document properties to confirm signature details such as the certificate authority, system product name, serial number, and the date/time stamp of creation. If the signature is a device signature, the name of the device that created the document is also included. A user signature, on the other hand, verifies the identity of the authenticated user who sent or saved the document.

In Device Signature PDF and Device Signature XPS modes, a digital signature is added using a certificate and key pair stored on the device. This allows recipients to verify the scanning device. If the optional Digital User Signature PDF Kit is enabled, users can install their own digital signatures. These signatures embed the user's name and email address, confirming the document's origin. Modifications to the document will also trigger a notification. To use Digital User Signature mode, user authentication via ULM or UA must be enabled, and a valid certificate must be installed on the device. Some models support only PDF format. Please refer to the Security Matrix for details.

Canon devices also support a feature called PDF Visible Digital Signature, which forces the digital signature to appear on the first page of the PDF file, making it visible without opening the document properties. Users can select the signature to be displayed from the [Scan and Send] screen. This not only makes the digital signature more prominent but also ensures it appears on printed versions of the document.

Send to Myself (Only)
Canon devices offer a document delivery solution called "Send to Myself (Only)." This feature allows administrators to configure the device so that users can scan and send documents only to their own email

address or personal folder. Because this function does not permit users to enter arbitrary email addresses when sending scanned documents, it is designed to help limit information leaks.
** Note: Folder and email information must be registered in the user account of the authentication system.*

Copy Set Numbering
Canon devices support the ability to add copy set numbers to printed or copied output in user-defined areas on the page. Copy set numbering provides a way to track documents based on the set number received by the recipient.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.2–Data Security features

This section describes the data security features on Canon devices.

3.2.1 Stored Data

Data Protection for HDD, SSD, and eMMC * Functionality varies by model.
Canon devices are equipped with Hard Disk Drive (HDD), Solid State Drive (SSD), or embedded Multi Media Card (eMMC) storage for data retention (the type of storage varies by product).

Canon devices include data erasure tools and encryption functions compatible with HDDs, SSDs, and eMMC storage.

Data Erasure *Functionality varies by model.
Select Canon devices are equipped with features to erase certain data stored on internal media. Depending on the model, the device may use HDD, SSD, or eMMC storage. For details, please refer to the Security Matrix.

Canon's HDD erasure functions are designed to help make data recovery more difficult. Users can select the desired erasure method based on the level of security required:

Available methods include:

- Single overwrite with null data (default)
- Single overwrite with random data
- Triple overwrite with random data
- Triple overwrite in the following sequence (DoD standard):
  - Fixed value
  - Complement of the fixed value
  - Random data
- Nine-time overwrite with random data

The DoD standard is a data clearing and sanitization method used to overwrite existing information on a hard drive.

For SSDs and eMMC, the erasure function also aims to make data recovery difficult by overwriting data with zeros.

Data erased when executing HDD/SSD erasure includes:
- Data stored in Box
- Address book entries
- Scan settings registered in the Send function
- Mode memory settings for Copy and Box functions
- MEAP applications
- Data saved via MEAP applications
- MEAP SMS (Service Management Service) passwords
  (If changed, the password will revert to factory default)

- User authentication credentials registered via local device authentication
- Unsent documents (e.g., scheduled or reserved transmissions)
- Job history information
- Settings configured via the initial setup/registration screen
- Registered forms for image composition
- Registered forwarding settings
- Registered key pairs and server certificates
- Unprinted documents (e.g., hold print jobs)

If MEAP applications are installed during erasure, the applications themselves will be deleted, but license information will remain on the device. To avoid this, be sure to deactivate the license via SMS (Service Management Service: Application Lifecycle Management) before performing erasure.

Data erased when executing eMMC erasure includes:
- Address book entries
- Scan settings registered in the Send function
- Unsent documents
- Job history information
- Settings configured via the initial setup/registration screen
- Registered forwarding settings
- Registered key pairs and server certificates
- Unprinted documents

When initializing an HDD/SSD, a report is generated that includes the device serial number, device name, erasure method, date/time of erasure, and firmware version. For devices equipped with HDD/SSD, executing [Initialize All Data/Settings] performs both overwrite erasure and encryption key regeneration for encrypted data.

Storage Data Encryption Function (HDD, SSD, and eMMC) *Functionality varies by model.
The storage data encryption function uses an encryption chip built into select Canon devices to encrypt the storage medium (HDD/SSD and eMMC). This function is always enabled and cannot be disabled. Each device uses a unique encryption key, so even if the storage is connected to another device, the data cannot be read.

eMMC Data Encryption *Functionality varies by model.
The eMMC data encryption function uses AES 128-bit encryption with the XTS mode.

HDD/SSD Data Encryption*Functionality varies by model.
The HDD/SSD data encryption function uses AES 256-bit encryption with the XTS mode.

FIPS 140-3 Level 2 Certification* Functionality varies by model.
The encryption chips used in HDD/SSD storage are certified to FIPS 140-3 Level 2 under the U.S./Canada Cryptographic Module Validation Program (CMVP).

Exceptions for HDD/SSD Data Encryption and FIPS certification* Functionality varies by model.
Certain models in the imageRUNNER ADVANCE series released before 2020 (e.g., iR-ADV DX C568/C478) use AES 256-bit encryption with CBC mode. The encryption chips in these devices are compliant with FIPS 140-2 Level 2, a U.S. federal information processing standard, and are certified under both the U.S./Canada Cryptographic Module Validation Program and Japan's Cryptographic Module Validation Program (JCMVP).

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.2.2 Job Log Concealment Function
Once turned on, the standard Job Log Concealment function is designed to prevent job history processed through the device from being displayed to general users on the main control panel or via the Remote UI. While job log information is hidden from general users, system administrators can still access it. Administrators can print the job log to review usage details for copy, fax, print, and scan operations on the device.

The default setting for Job Log Concealment is [Off].

3.2.3 Trusted Platform Module (TPM) *Functionality varies by model.

Once enabled, the Trusted Platform Module (TPM) is a tamper-resistant hardware security chip on select Canon devices that stores encryption keys used to help protect passwords, authentication keys, and other sensitive data within the device.

** Note: The TPM function is disabled by default.*
** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.2.4 HDD/SSD Password Lock *Functionality varies by model.

Select Canon devices include a feature called HDD (or SSD) Lock. This function helps protect the HDD/SSD with a password. If the HDD/SSD is physically removed from the device, the data cannot be accessed from a PC.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

3.3–Fax Security

This section describes the fax security features of Canon devices. The information applies only to models equipped with fax functionality.

3.3.1 Super G3 Fax Board Communication Mechanism

Select Canon devices are equipped with Super G3 fax functionality. The modem on the Super G3 fax board supports only fax modem functions and does not include data modem capabilities. As a result, TCP/IP communication over telephone lines is not possible. Additionally, there are no functional modules such as Remote Access Service that would enable communication between the telephone line and the device's internal network.

3.3.2 Fax Transmission

The PC Fax function allows users to send documents from a compatible PC via the network using a fax driver. However, the data transfer from the PC to the device over the network and the data transfer from the device to the telephone line via the G3 fax board are structurally separated.

3.3.3 Received Faxes

Fax boards that can be installed in Canon devices do not support binary file transfer via fax protocols. Therefore, it is not possible to receive non-image data files (such as files containing viruses). Even if a file disguised as a fax image containing a virus is received, the device attempts to decode it using fax encoding. This results in a decoding error, the line is disconnected, and the data is discarded by the device.

Select Canon devices include a built-in data storage feature called the Box function (also used for confidential fax reception). However, operations involving the Box via Publicly listed phone numbers are limited to storing image data only. The destination Box is determined by the device's forwarding settings. The data stored in the Box is in fax image format,. Furthermore, fax protocols that would allow viewing, deleting, or retrieving Box data via public telephone lines are not implemented.

3.3.4 Other Fax Features

Allow/Restrict fax transmission via the fax driver

Devices can be configured to either allow (default) or restrict fax transmission via the PC fax driver.

Allow/Restrict Transmission from History (Job Log)

Devices can be set to either allow (default) or restrict the use of the last three addresses, scan settings, and transmission settings during fax transmission.

Receiving Faxes to Storage

Canon devices can receive faxes into storage rather than immediately printing them to the output tray. Faxes can be stored in a memory inbox based on predefined conditions, allowing for later printing. These inboxes can be password-protected to help limit unauthorized access.

Fax Destination Confirmation * Functionality varies by model.

To help limit documents from being sent to incorrect fax numbers, select Canon devices offer a feature to confirm the entered fax number. When enabled by the administrator, users are prompted to re-enter the recipient's fax number before sending. If the numbers do not match, the user is asked to re-enter the original number for confirmation.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

Section 4 — Network Security

4.1– Network and Print Security

Canon devices are equipped with network security functions designed to help organizations in their efforts to protect information during printing and scanning over a network. These security functions allow access to the device and printing only by authorized users, restrict device communication to specified IP/MAC addresses, and enable control over the availability of individual network protocols and ports as needed. Additionally, to help organizations in their efforts to protect communication data, Canon devices support encryption technologies such as IPSec and TLS.

4.1.1 Enabling/Disabling Protocols/Applications * Functionality varies by model.

Network administrators can configure which device protocols and ports are accessible through the settings of select Canon devices. This is designed to so organizations can effectively block unwanted device communication and system access via specific transport protocols. Select Canon devices also offer the ability to disable unused TCP/IP ports to help enhance device security. Disabling ports may affect the availability of certain functions and applications on the device. The configurable ports are as follows:

Summary of Port Settings for Canon Devices

		imageRUNNER ADVANCE DX imagePRESS Lite imageFORCE except the models listed on the right side of this table		**imageFORCE C1300/1400 Series**	
Name	**Description**	**Port**	**Default**	**Port**	**Default**
TCP					
LPD	LPD print	515	ON	515	ON
RAW	RAW print	9100	ON	9100	ON
HTTP	World Wide Web HTTP	80	ON	80	ON
HTTPS	HTTP over TLS/SSL	443	OFF	443	ON
HTTP (MEAP)	World Wide Web HTTP for MEAP	8000	ON	-	-
HTTPS (MEAP)	World Wide Web HTTP for MEAP	8443	ON	-	-
SMTP	Simple Mail Transfer Protocol	25	OFF	25	OFF
IPP	Internet Printing Protocol	631	OFF	631	ON
FTP	File Transfer Protocol	21	OFF	21	OFF
NetBIOS-ssn	NetBIOS Session Service (SMB)	139	OFF	-	-
CPFS	CIFS	445	OFF	-	-
VNC	Canon VNC port	5900	OFF	5900	OFF
Remote FAX	Remote FAX	20317	OFF	-	-
WSDScan	WSDScan	60000	OFF	60000	OFF
SIP	TP FAX	5060	OFF	-	-
SIP REGIST (TLS)	IP FAX	5061	OFF	-	-
T38	IP FAX	49152	OFF	-	
UDP					
SNMP	SNMP	161	ON	161	ON

SLP	Service Location Protocol	427	OFF	427	OFF
WSD	WSD WS-Discovery	3702	OFF	3702	ON
IPsec	IPsec IKEvl	500	OFF	500	OFF
IPsec	IPsec IKEvl	4500	OFF	-	-
BML inkS	BML inkS Discovery	1900	OFF	-	-
mDNS	mDNS/mDNS-SD	5355	OFF	-	-
SIP	IP FAX	5060	OFF	-	-
RTP	IP FAX	5004	OFF	-	-
RTCP	IP FAX	5005	OFF	-	-
t38	IP FAX	49152	OFF	-	-

IP Address Filtering *Functionality varies by model.
Select Canon devices support IP address filtering.

To configure filtering, you need to set a default policy (either "Deny" or "Allow") and register the IP addresses to be excluded.

If the default policy is set to "Allow," you must register the IP addresses to be denied. Conversely, if the default policy is set to "Deny," you must register the IP addresses to be allowed. The default setting for both incoming and outgoing communication is "Allow."

> **Port Number Blocking Function *Functionality varies by model.**
> If the default policy is set to "Allow," specifying a port number will block communication to that port number from any IP address.
> If the default policy is set to "Deny," specifying a port number will allow communication to that port number from any IP address.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.2 Remote UI Login Timeout Setting *Functionality varies by model.

Select Canon devices allow administrators to configure the timeout period for user remote logins. The default timeout value and the range of configurable durations vary depending on the model.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.3 Media Access Control (MAC) Filtering

MAC address filtering enables administrators to control access from specific systems to Canon devices, as well as from Canon devices to specific systems. In environments where IP addresses are assigned using Dynamic Host Configuration Protocol (DHCP), MAC address filtering is designed to helps limit issues that may arise when a system is assigned a new IP address after a DHCP lease expires. Similar to IP address filtering, MAC address filtering allows access to be permitted or denied for specific addresses. The MAC addresses can be easily added, edited, or deleted via the Remote UI. MAC address filtering is processed before IP address filtering. Even if a system's IP address changes due to DHCP, access control can still be enforced based on its MAC address.

4.1.4 TLS

Transport Layer Security (TLS) is an encryption protocol used to connect to services over the internet and transfer data. Canon devices use TLS, an encrypted communication protocol, designed to help protect data during transmission to and from external systems. This is designed to help limit eavesdropping, tampering, and impersonation when accessing Canon devices from PCs and other equipment.

TLS Version Selection

Canon devices support TLS versions 1.0, 1.1, 1.2, and 1.3. Administrators can select the appropriate version based on the configuration of connected systems and their organizational security policies. To restrict the TLS versions available on Canon devices, administrators can set upper and lower limits for supported versions. This allows organizations to determine if they want older, potentially vulnerable versions of TLS to be excluded from use..

While TLS 1.0 and 1.1 are supported to ensure compatibility with legacy systems, they may be deprecated in the future. Please refer to the latest specifications for each model.

Encryption Algorithm Selection

Administrators can align IPSec and TLS encryption algorithms with their operational policies. For TLS communication, administrators can select from various encryption, key exchange, signature, and HMAC algorithms. The available algorithms vary depending on the supported TLS version.

"✓": Available

"-": Not available

Algorithm	TLS Version			
	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
Encryption Algorithm Settings				
AES-CBC (256-bit)	✓	✓	✓	-
AES-GCM (256-bit)	-	-	✓	✓
3DES-CBC	✓	✓	✓	-
AES-CBC (128-bit)	✓	✓	✓	-
AES-GCM (128-bit)	-	-	✓	✓
CHACHA20-POLY1305	-	-	-	✓
Key Exchange Algorithm Settings				
RSA	✓	✓	✓	-
ECDHE	✓	✓	✓	✓
X25519	-	-	-	✓
Signature Algorithm Settings				
RSA	✓	✓	✓	✓
ECDSA	✓	✓	✓	✓
HMAC Algorithm Settings				
SHA1	✓	✓	✓	-
SHA256	-	-	✓	✓
SHA384	-	-	✓	✓

4.1.5 IPSec

Canon devices support IPSec. The IP Security Protocol (IPSec) is a protocol used for encrypted communication over networks such as the internet. While TLS encrypts communication at the application

level (e.g., HTTP communication via web browsers), IPSec encrypts communication at the IP protocol level.

IPSec supports communication at the IP layer through packets within authenticated and encrypted data streams. Because traffic is encrypted, it cannot easily be read by parties other than the intended recipient. It also helps ensure that the traffic has not been altered in transit and originates from a trusted party, protecting against replay attacks. Canon devices support only transport mode for IPSec, meaning authentication and encryption are applied only to the data portion of IP packets.

IPSec uses Internet Key Exchange (IKE) for key exchange and transmits encrypted data using Authentication Header (AH) and Encapsulating Security Payload (ESP). Canon devices require configuration of IKE, AH, and ESP.

Key Exchange Protocol (IKE)

Management of keys is essential for authentication and encryption in IPSec communication. IKE (Internet Key Exchange) is the protocol used for this purpose. There are two versions of IKE: IKEv1 and IKEv2. Canon devices support IKEv1.

IKE allows configuration of authentication methods, hash algorithms, and encryption algorithms. Supported hash algorithms include HMAC-SHA2 (256-bit, 384-bit), and supported encryption algorithms include AES-CBC (128-bit, 192-bit, 256-bit).

There are two authentication methods available in IKEv1:
[Pre-Shared Key Method]
To use the pre-shared key method, both devices must be configured with the same pre-shared key (a keyword of up to 24 characters) in advance. This key is used for authentication during IPSec communication.

[Digital Signature Method]
To use the digital signature method, a key pair file and a certificate authority (CA) certificate file must be created in advance and installed on the Canon device via the Remote UI. This CA certificate is used to authenticate the IPSec communication destination.

Supported key pairs and CA certificates for digital signature authentication include:

- RSA and ECDSA algorithms
- X.509 certificates
- Key pairs in PKCS#12 format

Authentication and Encryption Algorithms
Canon devices support the following IPSec authentication and encryption algorithms:

- **AH (Authentication Header)**
  Adds authentication information as a hash value to the IP header. It is used for source authentication and tampering checks. Note that AH does not encrypt the payload (main data being transmitted).

- **ESP (Encapsulating Security Payload)**
  Provides tampering checks and encrypts the payload. Supported encryption for the payload includes AES-GCM (128-bit, 192-bit, 256-bit).

4.1.6 FTPS *Functionality varies by model.

Select Canon devices support FTPS as a transmission protocol when sending scanned documents or forwarding received faxes to an FTP server.

To help with the security of FTP transmission, Canon devices support FTPS as defined in RFC 2228 and RFC 4217, which uses TLS. When FTPS is specified as the destination, TLS communication is executed. If the connection fails, the process ends with error code #801. This allows FTP communication to be encrypted and used.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.7 SMB *Functionality varies by model.

Server Message Block (SMB) is a protocol primarily used for data communication between Windows-based systems and other systems. Select Canon devices support the SMB protocol. They offer an "SMB client function" to send scanned data to external SMB servers, and for models with an Advanced Box, a "server function" that allows the Advanced Box to act as an SMB server.

SMB supports versions 1.0, 2.0, 3.0, and 3.1. During communication, the device negotiates with the destination system to determine the appropriate SMB version to use. It is also possible to specify the SMB version manually. Additionally, SMB communication can use SMB signing.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.8 Authentication Protocols

Canon devices support a variety of authentication protocols for network communication. For compatibility with legacy systems, a wide range of protocols is supported. However, please select the appropriate authentication protocol based on your system environment and the required level of security.

"✓": Supported
"-": Not supported

	Plain	CRAM-MD5	LM	NTLMv1	NTLMv2	Kerberos	OAuth2.0
IFAX/SMTP AUTH	✓ (Plain/Login)	✓	-	✓*	-	✓	✓
SMB Send/Browse	-	-	✓	✓	✓	-	-
SMB Advanced Box	-	-	✓	✓	✓	-	-

*NTLMv1 is not supported on some models.

NTMLv2
NTLMv2 is a challenge-response authentication protocol used in Windows-based networks. It is intended to enhance security by having both the client and server generate challenges and use them to compute responses, which can make it more difficult for attackers to predict the response.

Kerberos
Kerberos authentication is a ticket-based protocol. It allows access to server resources (such as files on a file server) using tickets issued by an authentication server like Active Directory.

OAuth 2.0
OAuth 2.0 is an authentication framework defined in RFC 6749. It uses access tokens issued by an OAuth 2.0 authorization server to authenticate users and grant specific clients access to resources provided by a service. This protocol is commonly used for cloud services and cloud API calls.

4.1.9 Wireless LAN * Functionality varies by model.

Select Canon devices support wireless LAN, enabling use in wireless network environments. Wireless LAN functionality may be built-in or available as an optional feature depending on the model.

Wireless communication security features include support for open systems or shared keys using Wired Equivalent Privacy (WEP) encoding, WPA (Wi-Fi Protected Access) Personal (WPA-PSK) with TKIP or

AES encryption, WPA2-PSK with Advanced Encryption Standard (AES), and WPA3-SAE (Simultaneous Authentication of Equals). (Note: WPA3 support varies by model.)

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.10 IEEE 802.1X

Canon devices support IEEE 802.1X, a standard for restricting access from unauthorized network devices on both wired and wireless networks. This authentication standard provides authentication to devices connected to the network and establishes a point-to-point connection only upon successful authentication.

IEEE 802.1X is already supported by many Ethernet switches and is designed to help limit guest systems, unauthorized systems, or unmanaged systems from connecting to the network if they fail authentication.

4.1.11 Dual-Line Support *Functionality varies by model.

Select Canon devices are equipped with both wired LAN and wireless LAN interfaces, and can use both connections simultaneously. One can be designated as the primary line and the other as the secondary line. The following combinations are supported:

- Wired LAN as the primary line: Wireless LAN can be used as the secondary line
- Wireless LAN as the primary line: Wired LAN can be used as the secondary line
- Wired LAN as the primary line: A second wired LAN via USB-LAN adapter can be used as the secondary line

The following functions available on the primary line are not supported on the secondary line:
Gateway settings, DNS name resolution, IPv6 communication, Auto IP settings, and IPSec.

IEEE 802.1X is available on the secondary line for some models.

The secondary line allows access only for specific types of communication:

・SNMP・LPD・RAW・HTTP/HTTPS(TLS)・mDNS・IPP・DHCPv4・WSD

・CPCA (UDP 47545 and TCP 9013 for both sending and receiving)

Communication between the primary and secondary LANs is not possible in either direction. On Canon devices that support the secondary line feature, routing functionality—which enables data relay between two or more different networks—is disabled.
Therefore, terminals connected to the primary and secondary LANs, which are on different networks, cannot communicate with each other through the device. Requests from one network cannot be forwarded to another.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.12 SCEP (Simple Certificate Enrollment Protocol)

Canon devices provide management functions for key pairs (consisting of a public key and a private key used in public-key cryptography), CA certificates, end-entity certificates (digital certificates), and CRLs (Certificate Revocation Lists).

SCEP is a protocol for certificate management. It enables operations such as issuing, renewing, and deleting certificates for clients such as devices and applications.

Using SCEP, Canon devices can request certificate issuance from a certificate management server. This feature is useful for automatically updating device key pairs used by a large number of devices without requiring direct administrator intervention, thereby reducing administrative burden.

In environments where IEEE 802.1X communication is performed using device key pairs issued by an internal certificate management server, certificates may expire in a short period (e.g., a few months). In such cases, certificates can be updated at a specified time using a timer, rather than manually updating each certificate via the Remote UI.

Certificate Request Features:

- Communication settings, key certificate settings, and timer settings required for certificate requests can be configured via the Remote UI.
- The device generates a key pair and CSR (Certificate Signing Request) based on instructions from the Remote UI, sends a certificate request (in PKCS#7 format) to the SCEP server, and upon receiving the public key certificate, registers it as the certificate corresponding to the generated key pair.
- At the time specified by the timer, the device sends a certificate request to the SCEP server using the same method and registers the received certificate.

4.1.13 OCSP (Online Certificate Status Protocol)

Canon devices support OCSP (Online Certificate Status Protocol: RFC 6960), a protocol for checking the validity of X.509 certificates online. Using OCSP limits the need to manually update CRLs (Certificate Revocation Lists) that contain certificate revocation information.

4.1.14 Embedded Web Browser * Functionality varies by model.

On select Canon devices, the embedded web browser displays HTML content retrieved from a web server on the user interface of the device's control panel. This browser uses the "WebKit" rendering engine.

It supports basic authentication and digest authentication, and can display PDFs encrypted with AES 256-bit encryption.

The following security-related settings are also available:

- TLS version selection
- JavaScript enable/disable
- Display of mixed HTTPS/HTTP content

** Note: The embedded web browser is not available on all models.*
** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.1.15 SNMP

Canon devices support SNMP (Simple Network Management Protocol), a protocol used to monitor and manage network devices. SNMP allows retrieval and writing of MIB (Management Information Base) data over the network.

Canon devices support both SNMPv1 and SNMPv3. SNMPv1 allows access based solely on a community name (read-only or read/write access can be specified). SNMPv3 can help enhance security by providing user-based access control, source verification, tamper detection, and encrypted communication.

SNMPv1

SNMPv1 grants access to the device (read-only or read/write) using a simple string called the SNMP community string. Because access is granted using only a simple string, caution is advised when using this protocol. The default value is "public," but it is recommended to change this to a user-defined string for security purposes.

SNMPv3
SNMPv3 is designed to help protect against data tampering and enhance security by restricting access to authorized users through authentication and encryption. Use of SNMPv3 is recommended for improved security features.

4.2 Email Communication Security

4.2.1 Authentication Method

Canon devices can send and receive email requests via external mail servers. POP3 is used for receiving emails, and SMTP is used for sending. Both POP3 and SMTP support multiple authentication methods. These email communication functions are used in features such as iFAX and email sending.

By connecting Canon devices to external mail servers and enabling authentication during communication, security features can be implements surrounding email transmission and reception. In addition to supporting OAuth 2.0, Canon devices allow users to select an authentication method that matches their mail server configuration.

Canon devices support the following authentication methods:

Authentication methods available for both POP3 and SMTP:
- OAuth 2.0

Authentication methods available for POP3:
- APOP
- POP AUTH

Authentication methods available for SMTP:
- SMTP AUTH
- POP Before SMTP

It is recommended to enable TLS settings when using POP3 and SMTP protocols to encrypt communication.
To use encrypted communication, not only must TLS be enabled on the Canon device, but the connected mail server must also support the SMTP STARTTLS command (RFC 2487). If the mail server does not support STARTTLS, even with TLS enabled on the Canon device, the communication will be sent in plain text.

OAuth2.0 *Functionality varies by model.
OAuth 2.0 is an authentication method based on the OAuth 2.0 authorization framework defined in RFC 6749 and RFC 8628, commonly used for API integration in system environments. Instead of using a username and password for SMTP AUTH, OAuth 2.0 uses an access token issued by an OAuth 2.0 authorization server. This feature can be used when sending email (SMTP) via Microsoft Exchange Online and Google Workspace.
- For Microsoft Exchange Online, it uses the Device Authorization Grant as specified in RFC 8628.
- For Google Workspace, it uses the Authorization Code Grant as specified in RFC 6749.

** Note: POP Before SMTP, SMTP AUTH, and per-user SMTP authentication cannot be used simultaneously.*
** Note: Separate subscriptions to Microsoft Exchange Online and Google Workspace are required.*

APOP
APOP is a method that encrypts the password during email reception via POP3.

POP AUTH
POP AUTH is an authentication method using the SASL (Simple Authentication and Security Layer) mechanism defined in RFC 2222. It performs user authentication during POP connection to receive emails from registered users.

SMTP Authentication

SMTP AUTH is an authentication method using the SASL mechanism defined in RFC 2222. It performs user authentication during SMTP connection to send emails from registered users.

POP Before SMTP

This method authenticates with the POP3 server before sending via SMTP. If authentication is successful, the SMTP transmission is authorized.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

4.2.2 Antivirus Measures for Email Reception

Canon devices, in functions such as iFAX, can receive and process files attached to emails. Measures are in place to help limit the impact of virus-infected files during email reception.

For example, in iFAX reception, Canon devices support POP3/SMTP protocols for email reception. Upon receiving data, the email body and attachments are separated, and only image files in JPEG or TIFF format are printed and forwarded.

Three potential virus scenarios in email are addressed:

- **Virus attached to the email:**
  Attachments not in JPEG or TIFF format are immediately discarded upon receipt.

- **Viruses disguised as JPEG/TIFF files:**
  Canon devices compress the received JPEG or TIFF files, decode the image, and re-encode it. If processed successfully, the original image is discarded, and a new image is created, printed, and forwarded. If an error occurs during processing, the data is discarded, and an error message is printed in the email body.

- **Viruses embedded in email text:**
  Email data includes metadata such as "Date," "From," "Message ID," "To," and "Subject," followed by the message body. If binary virus data is embedded in the body, it is corrupted and discarded. If the virus is in a visible script format, the device processes the metadata first before handling the content.

Section 5 — Security Monitoring & Management Tools

Canon provides solutions to help organizations enforce their internal company policies and support their regulatory efforts. These solutions enable administrators to monitor the usage of Canon devices across the organization and allow the implementation of security policies to restrict access to device functions.

5.1– Security Policy Settings

As document, user, and information security is becoming more important to organizations, administrators need to be sure that the various settings are organized in a central location that can be password protected and managed. Canon provides features that allow administrators to centrally perform the following operations on Canon devices:

- Set passwords for access to security policy settings
- Access and review current security policy settings
- Edit and save changes to security policy settings
- Export security policy settings and push updates to other Canon devices

These features enable organizations to separate security management from device management. Once a password is created, device administrators will no longer have access to security policy settings.

5.2– imageWARE Enterprise Management Console

The imageWARE Enterprise Management Console (iW EMC) is a highly scalable web-based management utility for administrators that delivers a streamlined, centralized point of control for compatible devices installed across enterprises. iW EMC makes it easier for organizations to manage one or more compatible Canon devices remotely across a network. iW EMC allows configuration of device information, firmware updates, address book distribution, and application management using encryption.

5.3– Security Environment Estimation * Functionality varies by model.

5.3.1 Security Environment Estimation Function

Upon device setup, the MFP uses an estimation algorithm developed by Canon using machine learning and recommends one of the following six usage environment types based on the data obtained from the user's environment.

- Intranet And Internet Connection
- Direct Internet Connection
- Internet Connection Prohibited
- Private (Home) Network
- Public Network
- Highly Confidential Info. Environment

This function automatically assesses the office environment without requiring users to provide input or have prior knowledge of their security setup. To provide an environment estimation function, the printer estimates whether the communication tendency is closest to any environment type from the statistical information of the received packet.
The estimation process is triggered under the following conditions:

- When the network is initialized (the IP address is fixed)
- When starting environment estimation is instructed from the setting

Steps of the Environment Assessment:

1. The device starts receiving packets on the network at a specific time.
2. The device processes the packets into statistical information. Specific information such as IP address and MAC address is anonymized for processing and statistical data is created.

3. The printer uses statistics and an environment estimation model within the device to estimate whether the printer's environment is closest to one of the environment types, and then displays the recommended environment type in the UI.

No learning occurs on the installed device. An update of the environment estimation model in the device can be performed by a firmware update of the entire MFP. Since the data used by the printer for estimation processing is statistical information, personal information and confidential information are not used for estimation processing. The environmental estimation model was created based on device information collected under the e-maintenance contract and statistical information collected individually by Canon.

As noted elsewhere, Canon does not warrant that use of its security features or recommendations will prevent security issues. Customers should perform their own due diligence and consult with their security expert to determine what security features to implement for their organization.

5.3.2 Detection Function

It provides the function of change detection. To notify a user in a status line that the result of environment estimation in which the installation environment of a printer is estimated as different from the result of the previous time. It provides Internet connection detection, and a status line informs the user that the device is accessible from the Internet and that two-factor authentication is recommended. To provide a function of a wireless LAN encryption method warning. Notify the user in the status line that the user is connected to a wireless LAN access point with an insecure encryption method or no encryption.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

Section 6 — Logging & Auditing

Select Canon devices are equipped with an audit log feature that records certain device behavior. By monitoring and analyzing these audit logs, users can look to see where they need to repair configurations, and review operations.. Additionally, audit logs can be useful in helping administrators in their efforts to identify the potential cause of security incidents when they occur.

Canon's audit log function can be integrated with compatible Security Information and Event Management (SIEM) systems, which centrally manage logs from IT equipment such as network devices and PCs. This integration can enable the collection and auditing of MFP logs using the same framework as for network devices and PCs.

The method of log output varies depending on the Canon device model. Some models store logs locally while also outputting them to external services (such as SIEM or Syslog servers), while others output logs directly to external services without storing them on the device. There are also models that do not support the audit log function.

** Note: Third party SIEM system required. Subject to third party SIEM system terms and conditions. Canon cannot ensure compatibility with all third party SIEM systems.*

6.1- Audit Log * Functionality varies by model.

An audit log is a chronological sequence of audit records to automatically track actions undertaken by users, developers, and administrators for the system. These records can be used by administrators to monitor system usage to determine their compliance efforts with respect to applicable regulations, security standards, enterprise policies, etc., as well as to prove usage effectiveness as audit trails.

The following logs are available:

Log Type	Content
User Authentication Log	Logs related to user authentication status (login/logout, authentication success/failure), user information registration/modification/deletion managed by User Authentication, and role management (add/set/delete) in ACCESS MANAGEMENT SYSTEM.
Job Log	Logs related to the completion of copy, fax, scan, send, and print jobs.
Send/Receive Log	Logs related to sending and receiving operations.
Advanced Box Save Log	Logs related to saving files to Advanced Box, network (Advanced Box on other devices), or memory media.
Box Operation Log	Logs related to operations on data within Boxes, System Boxes, or Fax Boxes.
Box Authentication Log	Logs related to authentication status of Boxes, System Boxes, or Fax Boxes.
Advanced Box Operation Log	Logs related to data operations within the Advanced Box.
Device Management Log	Logs related to device startup/shutdown, configuration changes via settings/registration, and changes made through device information distribution. If a serviceperson changes user or security-related settings during inspection or repair, it is also recorded here.
Network Authentication Log	Logs recorded when IPSec communication fails.
Batch Export/Import Log	Logs recorded when settings are batch exported or imported.
Box Backup Log	Logs related to the backup of data in Boxes, System Boxes, Fax Boxes, Advanced Boxes, Hold queues, and registered forms for image composition.
Application/Software Management Operation Log	Logs of operations in the Service Management Service (SMS), software registration/updates, and MEAP application installer.
Security Policy Log	Logs related to the status of security policy settings.
Group Management Log	Logs related to the status of user group settings (registration/modification/deletion).
System Maintenance Log	Logs related to firmware updates, and backup/restore of MEAP applications.

Secure Print Log	Logs related to information and operation history of held print jobs.
Settings Synchronization Log	Logs related to the synchronization of settings.
Audit Log Management Function Log	Logs related to the start, end, and export of the audit log management function.

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

6.2- Audit Log Management * Functionality varies by model.

Audit Log Collection feature has 3 main functions:

1. Audit Log Management Function

By enabling the audit log function, audit logs are stored in the device's internal storage. Up to approximately 40,000 logs can be retained. When the number exceeds 40,000, older logs are deleted and replaced with new ones. It is also possible to delete all retained logs

2. Audit Log Export Function

Audit logs stored on the device can be exported as a CSV file. The export function includes both manual and automatic export options.

3. Audit log transmission via Syslog / SIEM integration feature

Certain customers use systems like Syslog or SIEM servers to collect system logs. Canon devices are capable of transmitting audit logs to many of these compatible systems

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

6.3- Audit Log Syslog Send Function

Canon devices have the capability to convert collected logs into the Syslog format and transmit them to a Syslog server. Audit logs generated within the device are sent to the Syslog server in real time. The format and processing flow of the transmitted Syslog messages comply with RFC5424, RFC5425, and RFC5426.

Communication with the Syslog server can be configured to use either the UDP or TCP protocol. When TCP is selected, encrypted communication using TLS is also available (off by default. Must be turned on). Devices that retain audit logs internally will continue to store them even after they are sent to the Syslog server.

Even models that do not retain audit logs internally can utilize the function to send audit logs to a Syslog/SIEM system in real time. In such cases, the audit logs are not stored within the device.

6.4- Audit Log SIEM Send Function

SIEM (Security Information and Event Management) is a system that collects and centrally manages logs from IT devices such as network equipment and PCs.

By aggregating and analyzing logs from multiple devices, SIEM systems can support corporate security operations in the following ways:

Detecting incidents and early warning signs
(By verifying logs from multiple devices in real time, SIEM can help users in their efforts to identify phenomena that may lead to incidents.)

Rapid root cause analysis after an incident
(Analyzing logs accumulated in the SIEM can help users in their efforts to identify the root cause of incidents.)

Reviewing security operations
(Regular log analysis by users makes it possible to visualize configurations or usage that deviate from established rules, enabling operational improvements.)

Canon devices have the capability of sending audit logs to compatible SIEM systems. This functionality allows Canon devices to be integrated into the centralized monitoring framework alongside other IT equipment such as network devices and PCs.

Canon devices support the standard Syslog format for sending logs to compatible SIEM systems. Since SIEM systems can receive logs in Syslog format, integration is possible. However, because each SIEM interprets and processes received log data differently, configuration on the SIEM side is required.
For more details, please refer to Canon's SIEM white paper.

** Note: Canon does not make any representation or warranty about any SIEM system. Third party SIEM system required. Subject to third party SIEM system terms and conditions. Canon cannot ensure compatibility with all third party SIEM systems.*

** Note: See the Security Matrix at https://partners.usa.canon.com/online/myportal/partners/home/security to determine if this feature is available for the model you are interested in. Please be sure to check back before purchasing, as specifications and availability are subject to change.*

Section 7 — Canon Solutions & Government Requirements

7.1- Common Criteria

The Department of Defense required a broad group of commercial hardware/software suppliers to have their products evaluated using a standard known as Common Criteria to determine its fitness for the department's use.

Following the development of the Common Criteria, the National Institute of Standards and Technology and the National Security Agency, in cooperation and collaboration with the U.S. State Department, worked closely with their partners in the CC Project to produce a mutual recognition arrangement for IT security evaluations that use the Common Criteria. The Arrangement is officially known as the Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security. It states that each participant will recognize evaluations performed using the Common Criteria evaluation methodology where product certificates have been issued by the Mutually Recognized producing nations for EAL1-EAL4 evaluations. Evaluation Assurance components found in EAL5-EAL7 are not part of the mutual recognition arrangement.

The list of Common Criteria Recognition Arrangement members currently includes Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Netherlands, New Zealand, Norway, Singapore, Spain, Sweden, Turkey, Malaysia, Pakistan, Qatar, United Kingdom and United States.

7.2- Common Criteria Certification

The Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408 Standard, defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. It specifies information security functional requirements and seven predefined assurance packages, known as Evaluated Assurance Levels (EAL), against which products' functions are tested and evaluated.

EAL provide both the vendor and user with flexibility to define functional and assurance requirements that are unique to their operating environments and to obtain an evaluated product best suited to those needs.

Hardware and software companies around the world use the Common Criteria (CC) evaluation program to provide a means of comparison for the level of assurance that their products provide. As a cautionary note, while the evaluation program is very effective at validating a manufacturer's claims, it does not measure the overall security capabilities or vulnerabilities as a whole. Therefore, Common Criteria certification should be one of many considerations when choosing security-related products instead of being considered the de-facto standard.

For the list of certified products, please access the link below.
Certified Products: CC Portal (commoncriteriaportal.org)

7.3- Hardcopy Device Protection Profile (HCD-PP)

HCD-PP (Hardcopy Device Protection Profile) was formulated in 2015 as the standard Protection Profile for the Japanese and U.S. governments' procurement of digital multi-function devices.
HCD-PP has more evaluation items related to cryptography than the conventional IEEE 2600. Specifically, management of cryptographic keys and document evaluation on entropy have been introduced, and cryptographic keys are properly managed and that random numbers generated have sufficient entropy.
HCD-PP is becoming mainstream for the Japanese and U.S. governments procurement requirements and bidding criteria for major corporations.

Unlike IEEE 2600, there will be no optional accessories required to comply with HCD-PP. Administrators need to change the device settings based on the Administrator Guide which will be available on the e-manual website (https://oip.manual.canon/). HCD-PP certification firmware installation by Canon authorized dealer service will also be required.

** Note: The manual is current as of the time that CC Certification (HCD PP) was obtained for the corresponding models. Refer to it in conjunction with the latest manual for your model.*

7.4- CAC/PIV Solutions for HSPD-12 Compliance

HSPD-12 requires the establishment of a standard for identification of Federal Government employees. The Presidential Directive calls for the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems.

Advanced Authentication (AA) CAC/PIV

AA CAC/PIV is a MEAP application which enables a user to authenticate to a MEAP enabled device via a Federal Government issued CAC or PIV card. AA CAC/PIV can also be used in conjunction with the Access Management System (AMS) limiting function access based on defined roles.

Authorized Send CAC/PIV

Designed to meet the needs of the United States Department of Defense and numerous government agencies, the Authorized Send CAC/PIV option for Canon devices provides a means for the devices to maintain high productivity for walk-up users to output hard copies of the documents they need while restricting access to the Send To features to users who have been authenticated using their Common Access Card (CAC) and/or Personal Identity Verification (PIV) card. This also supports a MEAP Log-in application using AMS for granular access control of ASEND functionality. This supports FIPS 140-2 validated cryptography and also integrates with AMS for device feature access control.

Section 8 — Conclusion

Canon devices continue to expand their functionality with each new model release, advancing their integration into IT and network infrastructures. Just like other networked equipment, printing devices must also be included in an organization's overall security strategy with respect to the confidentiality, integrity, and availability of information.

To meet the need for extensive and customizable security features for any environment, Canon devices offer a wide array of standard features and optional components. When properly deployed, these security features can be used in an organization's efforts to help protect devices. . Combined with advanced monitoring and management tools for auditing and centralized administration, the systems are designed to help meet the demand for increased productivity and security features.

As corporate privacy goals and regulations have become stricter, it is important to assess the level of security that all deployed imaging and printing devices provide. After careful review, existing devices may need to be either upgraded or replaced based on each unique environment.
Canon is committed to providing security features that can be used to help organizations with their critical information and is continually developing new technologies in this area. For more information on Canon devices, please visit https://www.usa.canon.com/business/workplace-security/device-security.

The information provided in this document is the most current information available at the time of its creation. Canon hereby expressly disclaims all warranties of any kind, express or implied, statutory or non-statutory, in relation to the information provided in this document.

In no event shall Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers be liable for any direct, special, consequential, incidental or indirect damages of any kind (including without limitation loss of profits or data or personal injury), whether or not Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers have been advised of the possibility of such damages, and Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers shall not be liable for any claim against you by a third party arising out of the use or performance of canon's products or information referenced herein.

Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its security features or recommendations will prevent malicious attacks, or prevent misuse of devices or data or other security issues. Customers should perform their own due diligence and consult with their security expert to determine what security features to implement for their organization. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment to ensure you understand their effects.

Trellix™ logos are registered trademarks of Trellix™. Canon, imageRUNNER, imageFORCE and imagePRESS Lite marks are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. uniFLOW is a registered trademark of NT ware Systemprogrammierung GmbH. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Specifications and availability subject to change without notice. Products shown with optional accessories. Additional information on software requirements and compatibility is available at usa.canon.com. Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitations, Sarbanes Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

The Trellix™ Embedded Control function is set to [Off] by default. It can be turned on by an administrator in Settings/Registration . When this function is set to ON, device startup will increase by 20 40 seconds (depending on the model). Recovery from Sleep Mode is not affected.

Third party SIEM system required. Subject to third party SIEM system terms and conditions. Canon cannot ensure compatibility with all third party SIEM systems. Not responsible for typographical errors.

Statements made in this document are the opinions of Canon U.S.A. None of these statements should be construed to customers or Canon USA's dealers as legal advice, as Canon U.S.A. does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

All specifications and availability are subject to change without notice.

www.usa.canon.com

Canon U.S.A., Inc.
One Canon Park
Melville, NY 11747