Canon Security Features Matrix

X = Included; O = Optional; – = Not Supported or Not Applicable

			imageFORCE			imagePRESS	imageRUNNER ADVANCE DX							
			MFP model		SFP Model		MFP Models							
FEATURE NAME		DESCRIPTION	imageFORCE C7165 C5170/C5160/C5150/C5140 C3150 8105/8195/8186 6170/6160/6150/6155 C611/C521/C431/C331 710/610/520	imageFORCE 1440F / C1333F	imageFORCE 1440P / C1333P	iPR Lite C265/C270	iR ADV DX C359iF C259iF	iR ADV DX C3935i C3930i C3926i	iR ADV DX C5870i C5860i C5850i C5840i	iR ADV DX C568iF C478iF	iR ADV DX 719iF 619iF 529iF	iR ADV DX 4945i 4935i 4925i	iR ADV DX 6980i	iR ADV DX 8905i 8995i 8986i
DEVICE SECURITY														
Authentication														
	Device Based													
	Universal Login Manager with uniFLOW Online	Provides login functionality before operating the device using Universal Login Manager (ULM) offered by 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. Multi-factor authentication support varies by model.	X	X	X	X	X	X	X	X	X	X	X	X
	User Authentication	UA allows login before device operation using users registered on the device, Active Directory/LDAP servers, or Entra ID (formerly Azure Active Directory). Also supports function-specific authentication.	X	–	–	X	X	X	X	X	X	X	X	X
	Department ID	Built-in feature 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. Functionality may vary by model.	X	X	X	X	X	X	X	X	X	X	X	X
	Active Directory Integration	The device integrates with Active Directory to perform authentication and retrieve user information.	X	–	–	X	X	X	X	X	X	X	X	X
	LDAP Server Integration	The device integrates with the LDAP server to retrieve information.	X	–	–	X	X	X	X	X	X	X	X	X
	Microsoft Entra ID Integration	The device integrates with Microsoft Entra ID to perform authentication and retrieve user information.	X	–	–	X	X	X	X	X	X	X	X	X
	Card Based													
	uniFLOW Card Authentication	When combined with the optional uniFLOW, Canon devices are able to securely 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 RFID Card Readers can also be integrated to support authentication using radio-frequency identification (RFID) cards.	O	O	O	O	O	O	O	O	O	O	O	O
	Advanced Authentication Proximity Card (AAProx)	Advanced Authentication Proximity Card enables support for an optional card reader on supported devices. Advanced Authentication Proximity Card is an embedded (serverless) MEAP application that lets you use existing HID proximity ID cards for device access and use. Administrators can leverage IDs stored locally on the device or Active Directory login via SSO-H.	O	O	O	O	O	O	O	O	O	O	O	O
	Advanced Authentication CAC/PIV	Advanced Authentication CAC/PIV enables support for an optional card reader on supported devices. Advanced Authentication CAC/PIV is an embedded (serverless) MEAP application that lets you use existing CAC/PIV cards for device access and use.	O	–	–	O	O	O	O	O	O	O	O	O
	Authorized Send for CAC/PIV	The Authorized Send CAC solution enables government agencies to distribute documents effectively and productively while limiting vulnerabilities through forced CAC authentication prior to sending hard-copy documents via the network.	O	–	–	O	O	O	O	O	O	O	O	O
	Control Cards/Card Reader System	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.	O	O	O	O	O	O	O	O	O	O	O	O
Access Control														
	Access Management System	The Access Management System, which is standard on 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. 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.	X	–	–	X	X	X	X	X	X	X	X	X
	Function Level Authentication	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.	X	–	–	X	X	X	X	X	X	X	X	X
	Password Protected System Settings	Password protects sensitive system settings so that only authorized users such as the administrator can make critical system wide changes.	X	X	X	X	X	X	X	X	X	X	X	X
	Scan and Send Security													
	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.	X	X	–	X	X	X	X	X	X	X	X	X
	Access Code for 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.	X	×	–	X	X	X	X	X	X	X	X	X
	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.	X	X	–	X	X	X	X	X	X	X	X	X
	Print Driver Security Features													
	Print Job Accounting	A standard feature in Canon' s printer drivers, print job accounting requires users to enter an administrator-defined password prior to printing, thereby restricting device access to those authorized to print. Printing restrictions can be set using Department ID credentials or through the Access Management System.	X	X	X	X	X	X	X	X	X	X	X	X

FEATURE NAME		DESCRIPTION	imageFORCE C7165 C5170/C5160/C5150/C5140 C3150 8105/8195/8186 6170/6160/6150/6155 C611/C521/C431/C331 710/610/520	imageFORCE 1440F / C1333F	imageFORCE 1440P / C1333P	iPR Lite C265/C270	iR ADV DX C359iF C259iF	iR ADV DX C3935i C3930i C3926i	iR ADV DX C5870i C5860i C5850i C5840i	iR ADV DX C568iF C478iF	iR ADV DX 719iF 619iF 529iF	iR ADV DX 4945i 4935i 4925i	iR ADV DX 6980i	iR ADV DX 8905i 8995i 8986i
	Custom Driver Configuration Tool	Administrators can create custom driver profiles for users to limit access to print features and specify default settings, thereby protecting the device against unauthorized use, enforcing internal policies and better controlling output costs. Security conscious settings that can be defined and enforced include duplex output, secure print, B&W only on color devices, watermarks and custom print profiles, as well as hiding any desired functions.	X	X	X	X	X	X	X	X	X	X	X	X
	USB Block	USB Block allows the System Administrator to help protect the imageRUNNER ADVANCE systems 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.	X	X	X	X	X	X	X	X	X	X	X	X
	Third Party MEAP Application Development	Canon actively collaborates with major software vendors to develop custom MEAP (Multifunctional Embedded Application Platform) applications. Each MEAP-compatible device includes safeguards to ensure the security and integrity of stored information. 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 for operability and security. Following the review, the application is digitally signed with a special encrypted signature to protect the integrity of the application. If the application is modified in any way, the signature code will not match and the application will not be permitted to run on the device. These safety measures make it virtually impossible for an altered or rogue MEAP application to be executed on a Canon device.	X	–	–	X	X	X	X	X	X	X	X	X
Others														
	Tamper Detection Feature (Verify System at Startup)	Once enabled, 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', enhanced security against software tampering is provided. Furthermore, standard cryptographic technologies (hash, digital signature) are used for verification.	X	X	X	X	X	X	X	X	X	X	X	X
	Platform Firmware Resiliency (Automatic Recovery)	The Platform Firmware Resiliency is firmware automatic recovery function. This feature will attempt to continue operation using the backup program without stopping the startup when an illegal program is detected by Verify System at Startup.	X	X	X	X	X	X	–	–	X	X	X	X
INFORMATION SECURITY														
Document Security														
	Secure Printing													
	Secured Print	This function reduces the risk of information leakage by requiring 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.	X	X	X	X	X	X	X	X	X	X	X	X
	Encrypted Secured Print	Canon devices enhance security by encrypting print data before transmitting it to the Canon print device. This function supports AES 256-bit encryption.	X	X	X	X	X	X	X	X	X	X	X	X
	uniFLOW Secure Print	Canon offers a secure printing 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 securely printing company data at home using a secure system and communication channel.	O	O	O	O	O	O	O	O	O	O	O	O
	Forced Hold	Canon devices can be configured to require hold printing. 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.	X	–	–	X	X	X	X	X	X	X	X	X
	Advanced Anywhere Print (AA PRINT)	Advanced Anywhere Print (AA-PRINT) is a serverless MEAP solution for Canon devices that combines the productivity of a print-anywhere solution with the security of login management. It enables user access control and job tracking without the need for a dedicated server. Users can securely print and release their jobs from any 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 ensure print security, reduce maintenance costs, and maximize productivity—without the need for additional servers or associated maintenance overhead.	×	–	–	O	O	O	O	O	O	O	O	O
	Document Storage Space Protection													
	Mail Box Security (password protection)	Mail Box Security is an onboard secure printing workflow. For example, a user can store print jobs to a password-protected Mail Box on the device. Later, that same user can walk up to the device and enter the Mail Box password to print the job as needed.	X	–	–	X	X	X	X	X	X	X	X	X
	Advanced Box Security (password protection)	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.	X	–	–	X	X	X	X	X	X	X	X	X
	Other Document Security Capabilities													
	Watermark / Secure Watermark	You can output your documents with hidden text embedded in the background. If a copy is made, the hidden text appears on the resulting pages, making clear that the copy is unauthorized.	X	X	X	X	X	X	X	X	X	X	X	X
	Encrypted PDF	In Encrypted PDF mode, security can be enhanced by encrypting PDF files sent to email addresses or file servers, setting passwords, and defining access permissions. Only users who enter the correct password can open, print, or modify the received PDF files.	X	X	–	X	X	X	X	X	X	X	X	X
	Digital Signature PDF (Device and User Signature)	With the Scan and Send function, a digital signature can be added to PDF or XPS documents to verify their source and authenticity. 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.	X	X Only for PDF	–	X	X	X	X	X	X	X	X	X
	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 helps prevent information leaks.	X	X	–	X	X	X	X	X	X	X	X	X

FEATURE NAME	DESCRIPTION	imageFORCE C7165 C5170/C5160/C5150/C5140 C3150 8105/8195/8186 6170/6160/6150/6155 C611/C521/C431/C331 710/610/520	imageFORCE 1440F / C1333F	imageFORCE 1440P / C1333P	iPR Lite C265/C270	iR ADV DX C359iF C259iF	iR ADV DX C3935i C3930i C3926i	iR ADV DX C5870i C5860i C5850i C5840i	iR ADV DX C568iF C478iF	iR ADV DX 719iF 619iF 529iF	iR ADV DX 4945i 4935i 4925i	iR ADV DX 6980i	iR ADV DX 8905i 8995i 8986i
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.	X	–	–	X	X	X	X	X	X	X	X	X
Data Security													
NIST 800-88 Purge level	Extreme protection against the risk of information leakage from remaining data – purge erases the encryption key for the encrypted data in SSD, then overwrites all data once with "0", and then erases them all. Purge-level data erasure is the recommended method in NIST SP800-88	X	–	–	X	X	X	X	X	X	X	X	X
Secure Data Erasure for SSD, and eMMC	Canon devices are equipped with features to erase data stored on internal media. Depending on the model, the device may use SSD, or eMMC storage. Canon's SSD erasure functions are designed to make data recovery significantly more difficult. Users can select the desired erasure method based on the level of security required. The erasure function also aims to make data recovery difficult by overwriting data with zeros.	X (SSD)	X (eMMC)	X (eMMC)	X (SSD)	X (SSD)	X (SSD)	X (SSD)	X (SSD)	X (SSD)	X (SSD)	X (SSD)	X (SSD)
Storage Data Encryption Feature (SSD, and eMMC)	The storage data encryption function uses an encryption chip built into Canon devices to encrypt the entire 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.	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (eMMC) AES (128 bit/XTS)	x (eMMC) AES (128 bit/XTS)	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2	x (SSD) AES (256 bit/XTS) FIPS140-3 level 2
Job Log Conceal Function	The standard Job Log Concealment function prevents job history processed through the device from being displayed 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.	X	X	X	X	X	X	X	X	X	X	X	X
Trusted Platform Module	The Trusted Platform Module (TPM) is a tamper-resistant hardware security chip that securely stores encryption keys used to protect passwords, authentication keys, and other sensitive data within the device. It safeguards this information from external threats such as data leakage or tampering.	X (TPM2.0)	– hardware not supported	– hardware not supported	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)	X (TPM2.0)
HDD/SSD Password Lock	HDD (or SSD) Lock feature protects the HDD/SSD with a password, making it difficult to access the data stored on the drive. If the HDD/SSD is physically removed from the device, the data cannot be accessed from a PC. Please refer to the compatibility matrix for supported models.	X	–	–	X	X	X	X	X	X	X	X	X
Fax Security													
Allow/Restrict Fax Driver Transmissions	Device can be configured to allow (default) or restrict sending fax transmissions via a PC Fax driver.	X	X	–	X	X	X	X	X	X	X	X	X
Receiving Faxes to Memory Storage	Canon devices can receive faxes into storage rather than immediately printing them to the output tray. Faxes can be stored in a secure memory inbox based on predefined conditions, allowing for later printing. These inboxes are password-protected to prevent unauthorized access.	X	X	–	X	X	X	X	X	X	X	X	X
Fax Destination Confirmation	Tohelp prevent documents from being sent to incorrect fax numbers, 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.	X	X	–	X	X	X	X	X	X	X	X	X
NETWORK SECURITY													
Network (for Canon main unit													
Enabling/Disabling Protocols/Applications	Network administrators can configure which device protocols and ports are accessible through the Canon device's settings. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked. Canon devices also offer the ability to disable unused TCP/IP ports to enhance device security. Disabling ports may affect the availability of certain functions and applications on the device.	X	X	X	X	X	X	X	X	X	X	X	X
IP Address Filtering	IP address filters can be used to allow or deny access to specific device or machine addresses. Administrators can manage addresses using the Remote UI interface and can limit access to devices with individual or consecutive IP addresses or ranges. Also, a range of IP addresses can be permitted while certain addresses within that range are rejected.	X	X	X	X	X	X	X	X	X	X	X	X
IP Address Filtering (Port Number Block)	Controls data reception on specified port numbers (allow or deny). Since port numbers can be specified in the IP address filtering feature, the default policy follows the IP address filtering settings.	X	–	–	X	X	X	X	X	X	X	X	X
Remote UI Timeout	Canon devices allow administrators to configure the timeout period for user remote logins. The default timeout value and the range of configurable durations may vary depending on the model.	X	X	X	X	X	X	X	X	X	X	X	X
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 helps avoid 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. Up to 100 MAC addresses can be registered, and they 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.	X	X max.32	X max.32	X	X	X	X	X	X	X	X	X
TLS Encryption	Transport Layer Security (TLS) is an encryption protocol used to securely connect to services over the internet and transfer data. Canon devices use TLS, an encrypted communication protocol, to protect data during transmission to and from external systems. This helps prevent eavesdropping, tampering, and impersonation when accessing Canon devices from PCs and other equipment.	X	X	X	X	X	X	X	X	X	X	X	X
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 organizational security policies. To restrict the TLS versions available on Canon devices, administrators can set upper and lower limits for supported versions. This allows older, potentially vulnerable versions of TLS to be excluded from use, thereby maintaining security.	X	X	X	X	X	X	X	X	X	X	X	X
IPsec Support	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.	X	X	X	X	X	X	X	X	X	X	X	X
FTPS Support	To enhance 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 securely.	X	-	–	X	X	X	X	X	X	X	X	X

FEATURE NAME	DESCRIPTION	imageFORCE C7165 C5170/C5160/C5150/C5140 C3150 8105/8195/8186 6170/6160/6150/6155 C611/C521/C431/C331 710/610/520	imageFORCE 1440F / C1333F	imageFORCE 1440P / C1333P	iPR Lite C265/C270	iR ADV DX C359iF C259iF	iR ADV DX C3935i C3930i C3926i	iR ADV DX C5870i C5860i C5850i C5840i	iR ADV DX C568iF C478iF	iR ADV DX 719iF 619iF 529iF	iR ADV DX 4945i 4935i 4925i	iR ADV DX 6980i	iR ADV DX 8905i 8995i 8986i
SMB Support 2.0/3.0/3.1	Server Message Block (SMB) is a protocol for sharing resources, such as files and printers, with more than one device in a network. Devices use SMB to store scanned documents into a shared folder.	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)	–	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)	X (2.0/3.0)	X (2.0/3.0)	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)	X (2.0/3.0/3.1)
Network Authentication: OAuth2.0	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.	X SMTP/POP	X SMTP/POP	X POP	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)	X SMTP/POP (Firmware version 3.18 or later)
Network Authentication: 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. Kerberos is considered more secure than NTLMv2.	SMTP/POP	LDAP	–	X	X	X	X	X	X	X	X	X
Network Authentication: NTLMv2	NTLMv2 is a challenge-response authentication protocol used in Windows-based networks. It enhances security by having both the client and server generate challenges and use them to compute responses, making it more difficult for attackers to predict the response.	SMB Send / SMB Browse	SMB Send / SMB Browse	–	X	X	X	X	X	X	X	X	X
Wireless LAN	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.	O WPA/WPA2/WPA3	X WPA/WPA2/WPA3	X WPA/WPA2/WPA3	X WEP/WPA/WPA2/WPA3	O WEP/WPA/WPA2/ WPA3	O WEP/WPA/WPA2/ WPA3	X WEP/WPA/WPA2/ WPA3	X WEP/WPA/WPA2/ WPA3	O WEP/WPA/WPA2/ WPA3	O WEP/WPA/WPA2/ WPA3	O WEP/WPA/WPA2/ WPA3	O WEP/WPA/WPA2/ WPA3
IEEE 802.1X (Wired/Wireless)	IEEE 802.1X is 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.	X	X	X	X	X	X	X	X	X	X	X	X
Dual LAN Support	Canon devices are equipped with both wired and wireless LAN interfaces, and can use both simultaneously. One can be set as the primary connection and the other as secondary. The available combinations depend on the device model.	X	–	–	X	X	X	X	X	X	X	X	X
Certificate SCEP	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 overhead.	X	X	X	X	X	X	X	X	X	X	X	X
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 eliminates the need to manually update CRLs (Certificate Revocation Lists) that contain certificate revocation information.	X	X	X	X	X	X	X	X	X	X	X	X
SNMP v3	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 enhances security by providing user-based access control, source verification, tamper detection, and encrypted communication.	X	X	X	X	X	X	X	X	X	X	X	X
Mail Server Security													
APOP	APOP is a method for receiving email via POP3 that encrypts the password during transmission.	X	X	X	X	X	X	X	X	X	X	X	X
POP Auth	POP Auth is an authentication method using the SASL (Simple Authentication and Security Layer) mechanism defined in RFC2222. It authenticates users during POP connection to receive emails from registered users.	X	X	X	X	X	X	X	X	X	X	X	X
SMTP Authentication	SMTP Authentication uses the SASL mechanism defined in RFC2222 to authenticate users during SMTP connection, allowing registered users to send emails.	X	X	–	X	X	X	X	X	X	X	X	X
POP Authentication Before SMTP	This method performs authentication with the POP3 server before sending via SMTP. If authentication succeeds, the same credentials are used to authorize SMTP transmission.	X	X	–	X	X	X	X	X	X	X	X	X
SECIROTY MONITORING & MANAGEMENT TOOLS													
imageWARE Enterprise Management Console	IW EMC makes it easier for organizations to securely manage one or more Canon devices remotely across a network. IW EMC allows secure configuration of device information, firmware updates, address book distribution, and application management using encryption.	X	X	X	X	X	X	X	X	X	X	X	X
Security Policy Setting	The security policy function is used to collectively configure the security-related settings into one security policy. These settings can be protected by a dedicated password to achieve a high-level of security. Administrators can implement policy settings that comply with the security policies of their company to restrict people, other than the Administrators, from using functions that do not comply with the policies, or from changing the setting values.	X	X	X	X	X	X	X	X	X	X	X	X
Security Environment Estimation	The Security Environment Estomation will give recommended printer security settings according to the device environment, established by the machine learning, scanniong the network environment. Apply recommended security settings using the "Recommended Settings by Environment" button on a device.	X	–	–	–	–	–	–	–	–	–	–	–
LOGGING & AUDITING													
Audit Log Syslog Send Function (SIEM Integration)	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.	X	X	X	X	X	X	X	X	X	X	X	X
Audit Log Management	Audit Log Collection feature has 3 main functions: 1.Audit Log Management Function 2.Audit Log Export Function 3.Audit log transmission via Syslog / SIEM integration feature	X	–	–	X	X	X	X	X	X	X	X	X
SECURITY COMPLIANCE													
HCD-PP (Hardcopy Device Protection Profile)	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.	X C7165 / C5170 / C5160 / C5150 / C5140 / 6170 / 6160 / 6150 / 6155 Other models pending	–	–	–	X	X	X	X	X	X	X	X

	FEATURE NAME	DESCRIPTION	imageFORCE C7165 C5170/C5160/C5150/C5140 C3150 8105/8195/8186 6170/6160/6150/6155 C611/C521/C431/C331 710/610/520	imageFORCE 1440F / C1333F	imageFORCE 1440P / C1333P	iPR Lite C265/C270	iR ADV DX C359iF C259iF	iR ADV DX C3935i C3930i C3926i	iR ADV DX C5870i C5860i C5850i C5840i	iR ADV DX C568iF C478iF	iR ADV DX 719iF 619iF 529iF	iR ADV DX 4945i 4935i 4925i	iR ADV DX 6980i	iR ADV DX 8905i 8995i 8986i
	FIPS 140-2 (IPSEC/CAC/PIV/HDD Encryption/TLS)	FIPS (Federal Information Processing Standard) 140-2 is the benchmark for validating the effectiveness of cryptographic hardware. If a product has a FIPS 140-2 certificate you know that it has been tested and formally validated by the U.S. and Canadian Governments and widely adopted around the world in both governmental and non-governmental sectors as a practical security benchmark and best practice.	X	–	–	X	X	X	X	X	X	X	X	X
	FIPS 140-2 (network)	FIPS (Federal Information Processing Standard) 140-2 is the benchmark for validating the effectiveness of cryptographic module. If a product has a FIPS 140-2 certificate you know that it has been tested and formally validated by the U.S. and Canadian Governments and widely adopted around the world in both governmental and non-governmental sectors as a practical security benchmark and best practice.	–	–	–	X	X	X	X	X	X	X	X	X
	FIPS 140-2 (storage)		X	–	–	X	X	X	X	X	X	X	X	X
	FIPS 140-3(network)	FIPS (Federal Information Processing Standard) 140-3 is the latest benchmark for validating the effectiveness of cryptographic module, an upgrade on the previous 140-2 standard.	X	–	–	–	–	–	–	–	–	–	–	–
	FIPS 140-3(storage)		X	–	–	X	X	X	X	–	X	X	X	X

***Compliant- All other imageRUNNER ADVANCE devices (except imageRUNNER ADVANCE C2030/C2020) when installed with HDD Erase & Encryption kits, AMS and IPsec board*

****Check Canon USA Website for latest Certification Status*