SECURITY MATRIX

✓ = Included; Opt = Optional; N/A= Not Supported or Not Applicable

FEATURE NAME		DESCRIPTION	imageRUNNER									i-SENSYS											i-SENSYS X				
			iR 1643iF 1643i	iR C1225iF C1225	iR C1335iF C1325iF	iR 2206	iR 2206iF 2206N	iR 2520	iR 2425 2425i	iR 2645i 2630i 2625i	iR C3125i	i-SENSYS MF740 Series	i-SENSYS MF640 Series	i-SENSYS MF540 Series	i-SENSYS MF440 Series	i-SENSYS LBP660 Series	i-SENSYS LBP620 Series	i-SENSYS LBP325x	i-SENSYS LBP220 Series	i-SENSYS LBP852Cx	i-SENSYS LBP710 Series	i-SENSYS LBP350 Series	i-SENSYS X C1127i Series	i-SENSYS X 1238i Series	i-SENSYS X C1127P	i-SENSYS X 1238P Series	i-SENSYS X 1643P
DEVICE SECURITY																											
AUTHENTICATION																											
	DEVICE BASED																										
	Universal Login Manager (ULM)	Universal Login Manager (ULM) is a Server-less solution offering simple login and usage tracking functionality. It is designed to provide a solution for organisations that require device authentication and simple usage tracking in a customizable, easy-to-implement solution. It delivers convenient user authentication through picture logins, User Name/Password, or optional proximity cards, and allows organisations the ability to manage access and costs by controlling individual users' access and usage.	✓	N/A	N/A	N/A	N/A	N/A	✓	✓	✓	✓ (MF764Cx only)	✓ (MF645Cx only)	✓	✓ (MF446x & MF449x only)	✓ (LBP664Cx only)	N/A	N/A	✓ (LBP228x only)	N/A	N/A	N/A	✓	✓	✓	✓	N/A
	Department ID	Department ID Management Mode is a built-in feature that serves as a basic form of device access management for administrators. Department IDs are numeric and are stored locally on the device to let your business control access to the device.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	User Authentication	User Management allows greater flexibility with device authentication than Dept. ID alone, supporting alphanumeric input. An email address can be associated with a User ID that automatically populates the Reply To field for sent documents. User IDs can be linked to Dept. ID to impose volume or access limitations for copy, scan, and print functions.	N/A	N/A	N/A	N/A	N/A	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Single Sign On (SSO)	Single Sign On is a user authentication function that can be easily integrated with an Active Directory network environment. Leveraging user accounts from Active Directory reduces the burden on network administrators and eliminates the need for users to remember another password.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓ (MF764Cx only)	✓ (MF645Cx only)	✓	✓ (MF446x & MF449x only)	✓ (LBP664Cx only)	N/A	N/A	✓ (LBP228x only)	N/A	N/A	N/A	✓	✓	✓	✓ (1238P Only)	N/A
	Single Sign On Hybrid (SSO-H)	SSO-H expands on Single Sign On (SSO) by adding the capability of direct authentication using the Kerberos* or NTLMv2 protocols. (*Replaced by User Authentication for imageRUNNER 2600 & 2425 Series)	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
Card Based																											
	uniFLOW Authentication	Combined with optional uniFLOW, Canon devices can securely authenticate users through contactless cards, chip cards, and PIN codes. The solution supports a variety of card types such as magnetic cards and HID proximity cards that can be customized to help any business streamline print costs while drastically reducing security concerns.	Opt	N/A	Opt	N/A	N/A	Opt	Opt	Opt	Opt	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	Opt (LBP664Cx only)	N/A	Opt	Opt (LBP228x only)	Opt	Opt	Opt	Opt	Opt	Opt	Opt (1238P only)	Opt
	Control Cards/Card Reader System	The optional Control Card/Card Reader system provides device access and usage management. 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. The optional Control Card/Card Reader system manages populations of up to 300 departments or users, depending on the model.	Opt	N/A	Opt	N/A	N/A	Opt	Opt	Opt	Opt	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Opt	Opt	N/A	N/A	N/A
Access Control																											
	Password Protected System Settings	Password protects sensitive system settings so that only authorized users such as the administrator can make critical system wide changes.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Access Management System	When using the Access Management System, IT administrators can configure device access for both individuals and groups on a feature-by-feature basis so that when the user authenticated the functions that they are restricted from using are grayed out.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Function Level Authentication	Function Level Authentication, a part of the Access Management System, can be set to require that users authenticate after selecting certain features, thereby granting or restricting access based on function. For example, Function Level Authentication can be set to restrict or allow access to the Send function, by requiring the user to authenticate prior to using the capability.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	USB Block	USB Block allows the System Administrator to help protect the system against unauthorized access through the built-in USB interface. Access to the device's USB interface or desktop access and the device's host mode for other USB devices can each be permitted or disabled.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Scan and Send Security																											
	Address Book Password	A PIN and/or password that can be set for an individual address book in order to control user access to specific address books and contacts.	✓ (PIN only)	✓ (PIN only)	✓ (PIN only)	N/A	✓ (PIN only)	✓ (PIN only)	✓	✓	✓ (PIN only)	✓ (PIN only)	✓ (PIN only)	✓ (PIN only)	✓ (PIN only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓ (PIN Only)	✓ (PIN Only)	N/A	N/A	N/A
	Access Code for Address Book	Require and access code for access to that address book in order for a user to makes changes such as add, delete or modify and existing address.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
	Destination Restriction Function	With Universal Send, administrators can limit send capability to preapproved e-mail addresses or domain names only. The feature can also be used to prevent employees from sending documents to specific destinations, and it can also restrict users from adding specific types of new destinations.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
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.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Custom Driver Configuration Tool	Administrators can create customer 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 control 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.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Others																											
	Tamper Detection Feature (Verify System at Startup)	Canon's devices provide robust security infrastructure/ security functions. Measures against malware/firmware tampering were implemented to help prevent against attacks by not accepting programs without a digital signature by Canon when updating firmware or installing applications. In order to further prevent data disclosure due to unknown attacks/springboard attacks, additional security enhancements have been implemented.	✓	N/A	N/A	N/A	N/A	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	X	N/A	N/A	N/A	✓	✓	✓	✓	✓
Document Security																											
	Secure Printing																										
	Forced Hold Print	Forced Hold Print lets users see only the jobs that were sent by them in the Job Hold queue in the "Print Menu" when Forced Hold (Reservation) Printing is enabled. With Forced Hold (Reservation) Printing, IT Administrators can help reduce the amount of wasted prints, by requiring users to release their jobs after submitting them to the printer, which can reduce the amount of uncollected printouts around the MFP.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Secure Print	Secure Print* lets users protect documents they send to print. Rather than print automatically, jobs are held securely at the MFP until released by the user entering the correct password. This step prevents documents from being left out in a device tray unattended. *Some models may require additional option(s) to allow activation of this function.	✓	✓	✓	N/A	✓	✓	✓	✓	✓												✓	✓	✓	✓	✓
	Encrypted Secure Print	For enhanced security, the document data itself can also be encrypted during transmission and storage when printed with Encrypted Secure Print.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Opt	N/A	Opt	Opt	Opt	N/A	N/A	N/A	N/A	Opt
	uniFLOW Secure Print *requires uniFLOW/ uniFLOW Online/ uniFLOW online Express	uniFLOW Output Manager enables you to increase security measures for device activity across your organisation. To prevent unauthorized persons from retrieving confidential printouts, jobs can be held at the uniFLOW Output Manager server until a user provides identification at a networked supported device. This way any user can print a secure job and then select where to retrieve the document.	Opt	N/A	Opt	N/A	N/A	Opt	Opt	Opt	Opt	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	Opt (LBP664Cx only)	N/A	Opt	Opt (LBP228x only)	Opt	Opt	Opt	Opt	Opt	Opt	Opt (1238P only)	Opt
	uniFLOW Online	uniFLOW Online is a cloud-based secure print management solution. It is designed to provide the benefits of device authentication, secure follow me printing and secure mobile printing. uniFLOW Online delivers the most secure cloud printing platform available, as all network print jobs stay securely within the customer's local network, never making their way past the customer's firewall, and are never stored in the cloud, ensuring that documents are always safe.	Opt	N/A	N/A	N/A	N/A	N/A	Opt	Opt	Opt	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	Opt (LBP664Cx only)	N/A	Opt	Opt (LBP228x only)	Opt	Opt	Opt	Opt	Opt	Opt	Opt (1238P only)	Opt
Other Document Security Capabilities																											
	Watermark	You can output your documents with a semi-transparent watermark such as [CONFIDENTIAL] or [COPY] over print data when printing. You can also create your own watermarks.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Encrypted PDF	The Encrypted PDF mode within the Scan and Send Security Feature Set enables users to encrypt, set password and define permissions for PDF files that are sent to an e-mail address or file server for enhanced security. Only users who enter the correct password can open, print, or change the received PDF file.	✓	Opt	Opt	N/A	N/A	N/A	✓	✓	✓	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Opt	Opt	N/A	N/A	N/A
	Digital Signature PDF - Device	Within Universal Send, users can add digital signatures that verify the source and authenticity of a PDF or XPS document. When recipients open a PDF or XPS file that has been saved with a digital signature, they can view the document's properties to review the signature's contents including the Certificate Authority, system product name, serial number and the Time/Date stamp of when it was created. If the signature is a device signature it will also contain the name of the device that created the document, while a user signature verifies the identity of the authenticated user that sent or saved the document.	✓	Opt	Opt	N/A	N/A	N/A	✓	✓	✓	Opt (MF764Cx only)	Opt (MF645Cx only)	Opt	Opt (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Opt	Opt	N/A	N/A	N/A
	Digital Signature PDF - User	The Device Signature PDF and the Device Signature XPS mode use the device signature certificate and key pair inside the machine to add a digital signature to the document, which enables the recipient to verify the device that scanned it. If the optional Digital User Signature PDF kit is activated, users can install a digital signature that embeds their name and e-mail address to confirm their identity as the source of the document and provides notification if changes have been made. In order to use Digital User Signature Mode, SSO authentication must be enabled and a valid certificate installed on the device.	N/A	N/A	N/A	N/A	N/A	N/A	Opt	Opt	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Data Security																											
	Job Log Conceal Function	The standard Job Log Conceal function ensures that jobs processed through the device are not visible to a walk up user or through the Remote UI. The Job Log information although concealed, is still accessible by the administrator, who can print the Job Log to show copy, fax, print and scan usage on the device.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	eMMC - Memory Data Storage Security	Some of Canon devices use embedded MultiMediaCard (eMMC) mass storage devices that use NAND-based flash memory instead of a built-in hard disk drive (HDD). PCB mounting without PIN feet (BCA) and Flash memory sealing are implemented to reduce the risk of critical data loss at the printer. To further protect data encryption by the device firmware is performed when writing any data to the memory media.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Fax Security																											
	Super G3 Fax Board																										
	Prohibit PC-FAX	Prohibit the user from sending faxes via the device fax board from their PC. The PC Fax function can fax documents from the PC via Network, using a fax driver that runs on the PC. However, data transfer from the PC via Network to the device and data transfer (FAX transmission) from the phone line via the G3 FAX board is structurally separated.	✓	✓	✓	N/A	✓	N/A	✓	✓	✓	✓ (MF764Cx only)	✓ (MF645Cx only)	✓ (MF543 only)	✓ (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓ (C1127iF only)	✓ (1238iF only)	N/A	N/A	N/A
	Fax Received Notification	Similar to the Fax Forwarding function, the capability to define separate forwarding rules based on the line upon which the fax was received. Each fax can be routed to a specific shared or personal space, database, file server, Confidential Fax inbox or another fax device. When used in conjunction with the Job Forwarding to Advanced Box function, the Fax Received Notification feature sends an e-mail to designated recipients to immediately alert them of a new fax.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	✓ (MF764Cx only)	✓ (MF645Cx only)	✓ (MF543 only)	✓ (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓ (C1127iF only)	✓ (1238iF only)	N/A	N/A	N/A
	Fax Forwarding	The capability to define separate forwarding rules based on the line upon which the fax was received.	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Fax Destination Confirmation	To help prevent faxed documents from being inadvertently sent to the wrong destination, Confirm Entered Fax Number feature for additional protection. When enabled on the device by an administrator, users will be prompted to re-enter the recipient's fax number prior to sending in order to confirm that it matches the original one specified. If the fax numbers do not match, the user will be prompted to enter the original number again and re-confirm.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓ (MF764Cx only)	✓ (MF645Cx only)	✓ (MF543 only)	✓ (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓ (C1127iF only)	✓ (1238iF only)	N/A	N/A	N/A
	Fax Memory Lock	To prevent received faxed documents from automatically printing and collecting on an output tray, Fax Memory Lock holds incoming faxes in memory. Memory Lock can be enabled at all times, or only for times when the device is unattended (such as a lunch hour, or after business hours). Fax jobs can be released individually or collectively when Memory Lock is turned off.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓ (MF764Cx only)	✓ (MF645Cx only)	✓ (MF543 only)	✓ (MF446x & MF449x only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓ (C1127iF only)	✓ (1238iF only)	N/A	N/A	N/A
Fax Storage Space																											
	Fax In Box Security	Incoming faxes can be automatically routed to a designated Fax In Box, which can be password-protected to prevent the contents from being viewed by unauthorized individuals.	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NETWORK SECURITY																											
Network (for Canon main unit Only)																											
	Port Management	Through Canon's device setup and installation utilities, network administrators are provided with the ability to configure the specific device protocols and service ports that are accessible. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked.	✓	✓	✓	N/A	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	N/A	✓	✓	✓	✓	N/A
	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.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Media Access Control (MAC) Filtering* *not available on Wi-Fi"	MAC address filtering is useful for smaller networks where administrators can manage controls for specific systems, regardless of the subnet to which they happen to be connected. For environments using Dynamic Host Configuration Protocol (DHCP) for IP address assignments, MAC address filtering can avoid issues that are caused when DHCP leases expire and a new IP address is issued to a system. As with IP address filters, MAC address filters can be used to allow or deny access to specific addresses.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	TLS Encryption	Data transmission methods that can use SSL encryption include IPP, Internet-fax and Remote UI.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IPv6 Support	IPv6 support provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	SMB 1.0 Support	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.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
	SMB 2.0 Support	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.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
	SMB 3.0 Support	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.	✓	N/A	N/A	N/A	N/A	N/A	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
	TLS Version Selection	Administrators can specify TLS versions for encrypted communication. Previously, TLS 1.0, 1.1, and 1.2 were all enabled, but now both a version upper limit and version lower limit can be specified to restrict the available protocol versions. If vulnerability is discovered in an old version(s) of TLS, the administrator can disable that version in the device to help maintain security.	✓	N/A	N/A	N/A	N/A	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Cipher Algorithm Selection	Ability to enable/disable encryption and signing algorithms, such as 3DES (may apply to financial and government agencies), to help increase the strength of data encryption. Administrators can choose to only allow 256-bit for AES Key Length.	✓	✓	✓	N/A	N/A	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Wireless LAN	Wireless networking achieved through the installation of an optional Wireless LAN Board. The Wireless LAN Board is IPv6 compliant and supports the latest wireless traffic encryption standards, including WEP, WPA and WPA2, in addition to support for the IEEE802.1X authentication standard.	✓	N/A	N/A	N/A	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	✓	N/A	N/A	N/A	✓	✓	✓	✓	N/A
	IEEE 802.1X (Wired/ Wireless)	IEEE 802.1x is a standard protocol for port based Network Access Control. The protocol provides authentication to devices attached to a LAN port and establishes a point-to-point connection only if authentication is successful. The Extensible Authentication Protocol (EAP) is attached to both wired and wireless LAN networks, allowing multiple authentication methods such as cards and one-time passwords.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ (Wired only)	✓	✓ (Wired only)	✓ (Wired only)	✓ (Wired only)	✓	✓	✓	✓	✓ (Wired only)
	Audit Log Syslog Send Function (SIEM Integration)	Audit Log Collection feature has a function to convert the collected log to Syslog format and send to Syslog server. Format and process flow of Syslog to be sent conform to RFC5424, RFC5425 and RFC5426. Events for which Syslog Send is made are the ones to obtain audit log.	✓	✓	✓	N/A	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	SNMP v3	Simple Network Management Protocol (SNMP) is a protocol for monitoring and controlling communication devices in a network by using Management Information Base (MIB). Canon devices support SNMP v3, which provides greater security by protecting data against tampering, ensuring access is limited to authorised users through authentication and encrypting data sent over a network.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mail Server Security																											
	SMTP Authentication	To prevent unauthorized users from making use of the device's internal SMTP server, administrators can enable SMTP Authentication and designate a username and password to connect to the server. In addition, administrators can enable SSL for all SMTP send and receive operations.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
	POP Authentication Before SMTP	As an additional layer of security, administrators can enable or disable the POP Authentication before SMTP feature. POP Authentication before SMTP forces a successful login to a POP server prior to being able to send mail via SMTP.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
Others																											
	iW Enterprise Management Console (iW EMC)	The iW EMC monitors the device status you a complete record of activity on all network output devices from one Web-based location.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Device Configuration Management Plug-in	Allows administrators to configure device and interface settings as required and push the settings out to multiple devices. Provides the ability to back-up or restore detailed device settings to help save significant time and resources for IT departments.	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Restricting Device Setup Screens	Administrators can lock-out access to device setup screens for unauthorized users from the control panel and Remote UI utility in an effort to protect its configuration information.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LOGGING & AUDITING																											
	Restricting Device Setup Screens	iW MC Accounting Management Plug-in also provide a detailed audit trail of device activities for security purposes. Tracker generates activity logs that can provide insight into how each employee is using a single device.	Opt	N/A	N/A	N/A	N/A	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt	Opt

The information provided in this document is as available at the time of its creation.
All specifications and availability are subject to change without notice.

Edition No.1, Sep 2020