



WHITEPAPER:

imageRUNNER ADVANCE AND
imageRUNNER ADVANCE DX SECURITY

Canon

INTENT OF THIS DOCUMENT

Canon recognizes the importance of information security and the challenges that your organization faces. This white paper provides information security facts for Canon Multi Function Devices (MFD) imageRUNNER ADVANCE / imageRUNNER ADVANCE DX / imagePRESS C165 systems (hereafter called imageRUNNER ADVANCE). It provides details on imageRUNNER ADVANCE 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 imageRUNNER ADVANCE systems. The information in this document may be used to more clearly understand the many imageRUNNER ADVANCE security-related configuration capabilities offered by Canon. The imageRUNNER ADVANCE system offers a number of standard and optional capabilities that, when used by a customer, can help facilitate effective management and security of data processed and stored by the system. Ultimately, it is the customer's responsibility to select the method(s) most appropriate for securing their information.

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

Products shown with optional accessories/equipment. The features reviewed in this white paper include both standard and optional solutions for imageRUNNER ADVANCE systems. Specifications and availability subject to change without notice.



Contents

Introduction	2
Device Security.....	5
Data Security.....	17
Network Security.....	32
Security Monitoring & Management	47
Logging & Auditing.....	49
Canon Solutions & Regulatory Requirements	52
Conclusion.....	54
Appendix.....	55
Disclaimer	61

01

Introduction

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 to adequately protect information and assets from threats from the outside as well as within.

Nearly every day 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 MFDs, to the networks that connect them all.

As if the risks to computers, networks and devices weren't difficult enough to address, increased governmental regulations add an additional layer of strict compliance standards that must be met. Legislation such as the General Data Protection Regulation and Sarbanes-Oxley Act (SOX), Financial Conduct Authority (FCA) all require that IT administrators ensure the confidentiality, integrity and availability information receives the utmost attention.

Imaging & Printing Security Overview

Any networked Multifunction Device is potentially at risk of being attacked through the network. For this reason, MFDs require security measures just like PCs. Techniques of malicious adversaries evolve every day, and it is required not only to take actions against existing attack methods but also to provide a multi-layered defence with multiple proactive protection methods. Furthermore, because an MFD is also a document handling device, in addition to IT device security measures, document-specific security measures such as preventing printout leakage is also required.

The Canon imageRUNNER ADVANCE Security White Paper has been designed to provide detailed information on how imageRUNNER ADVANCE systems can address a wide variety of security concerns. Canon imageRUNNER ADVANCE systems offer many standard security capabilities, as well as a number of advanced security options that may be added for a higher level of confidentiality, integrity and availability of your mission critical information.

Canon continues to take information security measures to gain customer's trust and to be proactive in acquiring and maintaining third-party accreditation.

01 Introduction

Key Security Concentration Areas

Canon recognizes the vital need to help prevent data loss, protect against unwanted device use, and mitigate the risk of information being compromised. As a result, all imageRUNNER ADVANCE systems include many standard security features to help safeguard information. Canon imageRUNNER ADVANCE security capabilities fall into five key areas:

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

NOTE: Please refer to Table 9.2 in Appendix for the Security Features Table illustrating Device compatibility, and where a feature is standard or optional on the device.

Canon dedicates a significant amount of time and resources to continually improve the security capabilities of its imageRUNNER ADVANCE devices. Numerous robust 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.



Document Security

- Forced Hold Printing
- Send to Myself (only)
- Document Scan Lock and Tracking***
- Adobe® LiveCycle Rights® Management ES2
- Encrypted Secured Print**
- Watermark / Secure Watermark**
- Copy Set Numbering
- Encrypted PDF (AES 256 Support)**
- Digital Signature PDF**
- Fax Forwarding
- Fax Destination Confirmation

Mail Server Security

- POP Authentication before SMTP
- SMTP Authentication

Data Security

- Trusted Platform Module
- HDD Data Encryption
- FIPS 140-2 Validated HDD Encryption chip, IPsec, TLS, and CAC Card Authentication
- HDD Data Erase
- HDD Data Erase Scheduler (Opt.)
- HDD Initialize with report (up to 9 times overwrite)
- HDD Password Lock
- Advanced Box Security
- Mail Box Password Protection
- Job Log Conceal
- Removable Hard Disk Drive (Opt.)†

Network Security

- SMB 3.0 Support
- TLS Version Selection (up to v1.3)*****
- Cipher Algorithm Selection (includes disabling 3DES)
- IP/MAC Address Filtering
- IP + Port Filtering
- SSL Encryption
- Network Application On/Off
- USB Port On/Off
- Destination Restriction
- IPsec
- **FTPS Support*******
- Auto Certificate Update
- IEEE802.1X (Wired/Wireless)
- Dual-Line network (Opt.)
- NTLM Protocol Version Selection for SMB Connection
- **OSCP (Online Certificate Status Protocol)*******

Security Management

- Security Policy Settings
- SIEM Integration (Syslog Send)

Device Security

- Verify System at Startup*
- McAfee Embedded Control*
- IEEE2600 Common Criteria Certification (Opt.)

Logging/Auditing Security

- imageWARE Secure Audit Manager (Opt.)
- imageWARE Secure Audit Manager Express (Opt.)

Authentication

- Department ID
- Control Card Systems (Opt.)
- Universal Login Manager
- User Authentication
- uniFLOW/uniFLOW Online (Opt.)
- uniFLOW Online Express
- Device Level Log-in
- Active Directory Log-in
- LDAP Server (Lotus Domino and Novell eDirectory) Log-in
- Access Management System
- Function Level Log-in via AMS
- Authorized Send (Opt.)
- Smart Card Authentication (Opt.)
- Advanced Authentication-Proximity Card (Opt.)
- **Remote UI Default Password Change*******

01

Introduction

Note:

Depending on the model, some features are within the standard feature set of the device, while others require additional accessories. Document Scan Lock and Tracking^{***}, Encrypted Secure Print, Secure Watermark Encrypted PDF^{**}, Fax, Control Card System, Removable HDD^{***}, HDD Data Erase Scheduler, and IEEE2600 Common Criteria Certification are available as options. IEEE2600 Common Criteria Certification may not be available at time of launch. Check the price list for availability.

*Only available with 3rd edition models and imageRUNNER ADVANCE DX models. McAfee Embedded Control requires Unified Firmware Platform v3.9 or later

**Standard with DX models, 3rd edition and 2nd edition models. Optional with 1st edition models.

***Not available on imageRUNNER ADVANCE DX models.

****Standard with DX models. Available on 3rd edition, 2nd edition and 1st edition models with Unified Firmware Platform V3.10.

†There is no Removable HDD Kit option for DX models, but DX models (excluding C3700 Series) can have their HDD removed. When the connector reaches its service life, it must be purchased and replaced by a service technician.

02

Device Security

imageRUNNER ADVANCE Controller Security

The imageRUNNER ADVANCE series is built upon a platform that provides powerful enhancements to security and productivity. The architecture centres on an operating system powered by an embedded version of Linux, which is quickly becoming the most widely adopted platform for sophisticated devices. The source version used by imageRUNNER ADVANCE devices has been hardened by removing all unnecessary drivers and services so that only the ones essential to its operation are included.

The nature of embedded Linux and the hardening of the operating system drastically reduce the exposure to exploits as compared to a desktop or server version of a Linux or Windows operating system. Canon strives to develop products that meet or exceed our customer's security requirements. Some of the security related activities include independent testing by security consulting companies of Canon imageRUNNER ADVANCE devices during various phases of the development process to flush out any potential vulnerability prior to production. Also, Canon has collaborated with industry initiatives, such as the development of the IEEE 2600 CC Certification standards for hardcopy device and system security.

Authentication

Canon imageRUNNER ADVANCE systems include a number of authentication options which administrators can use to ensure that only approved walk-up and network-based users can access the device and its functions, such as print, copy and Scan and Send features. Beyond limiting access to only authorized users, authentication also provides the ability to control usage of colour output, and total print counts by department or user.

Device-Based Authentication

uniFLOW Online Express

uniFLOW Online Express is a server-less and Cloud-based login application for imageRUNNER ADVANCE devices (standard on third generation imageRUNNER ADVANCE), which provides an easy and convenient solution for user authentication. Ideal for small to medium size businesses, uniFLOW Online Express' simple user authentication includes card log-in (requires an additional option), PIN code, or user name and password, using local or Active Directory (AD), with minimal IT requirements. Utilising AMS (Access Management System), found on all imageRUNNER ADVANCE devices, uniFLOW Online Express allows comprehensive control of access on a per-user basis. In addition, uniFLOW Online Express delivers simplified tracking, allowing organizations to obtain a simple overview of user or device usage activity.

02

Device Security

User Authentication (UA)

The User Authentication (UA) is a new Multifunctional Embedded Application Platform, known as MEAP, login service which is available on the imageRUNNER ADVANCE C3300 Series, third generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165 model. User Authentication combines the SSO-H and Department ID functions available on other imageRUNNER ADVANCE Models. UA can manage up to 5,000 user accounts within 1,000 department codes.

Department ID Mode

An embedded feature within imageRUNNER ADVANCE systems, the Department ID Management mode permits administrators to control device access. If Department ID authentication is enabled, end users are required to enter a four-digit password before they are able to access the device. Up to 1,000 Department IDs can be configured and each can be configured with device function limitations, such as limiting, printing, copying and access to Advance Boxes, Mail Boxes and facsimile.

Access to Advanced Boxes, Mail Boxes, and Scan and Send (if applicable) can each be turned “On” or “Off” from the Limit Functions screen located under Department ID Management.

The settings can be made under Settings / Registration > Management Settings > User Management > Department ID Management

Single Sign-On Hybrid (SSO-H) Login

Single Sign-On Hybrid (SSO-H) is a Multifunctional Embedded Application Platform (MEAP) login service that can be used stand-alone with user data registered locally on the device or in conjunction with an Active Directory (AD) network environment. SSO-H supports the following modes:

- Local Device Authentication - with credentials stored in the device
- Domain Authentication - in this mode, user authentication can be linked to an Active Directory environment on the network
- Domain Authentication + Local Device Authentication

When used in Domain Authentication mode, a user must successfully authenticate using valid credentials on the system’s control panel, Remote UI utility, or web browser when accessed via a network prior to gaining access to any of the device functions.

02

Device Security

SSO-H ships as standard with MEAP capable imageRUNNER ADVANCE systems* and can support up to 200 trusted domains plus the users that belong to the same domain as the device. Canon imageRUNNER ADVANCE systems also ship with SSO-H, which supports direct authentication against an Active Directory domain using Kerberos or NTLMv2 as the authentication protocol. SSO-H does not require any additional software to perform the user authentication as it is able to directly communicate with the Active Directory domain controllers. In Local Device Authentication mode, SSO-H can support up to 5,000 users. For a combined use of Domain Authentication and Local Device Authentication, an LDAP server can be configured instead of Domain Authentication.

*This feature is not pre-packaged on third generation imageRUNNER ADVANCE models, imageRUNNER ADVANCE DX and imagePRESS C165.

Card-Based Authentication

uniFLOW Card Authentication

When combined with the optional uniFLOW, imageRUNNER ADVANCE systems 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 RF Ideas Card Readers can also be integrated to support authentication using radio-frequency identification (RFID) cards.

Access Control

Canon imageRUNNER ADVANCE systems support a number of access control options to help you manage the use of device settings and functions in addition to specific capabilities of certain functions. Canon offers solutions that can lock down the entire device, or simply lock down specific functions (e.g. Send-to-Email), while leaving other applications available for general use. With the power and flexibility of MEAP, some solutions can be customized to meet your specific requirements.

Access Management System

The Access Management System, which is standard on imageRUNNER ADVANCE systems, 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.

02 Device Security

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. Since the administrator is not limited to restricting all or none of a particular function, the roles can be as specific as is required for a number of business needs. Beyond the Base roles which contain default access restrictions, up to 100 new Custom roles can be registered for up to 5,000 users (when user is used). The administrator can also define whether to allow unregistered users to log in as guests and then specify settings for guest user's roles. The following describes the various Base access levels (roles) that are available:

Privileges by Access Level	
Predefined Role	Access Privileges
Administrator	Given privileges to operate all device functions.
Network Manager/Admin	Network manager mainly manages the settings related to the network under Settings/Registration.
Device Manager/Admin	Device Manager can specify settings related to management settings for paper type and function settings for Send/Receive.
Power User	Given privileges to operate all device functions, except managing the device itself.
General User	Given privileges to operate all device functions, except managing the device itself and specifying/registering address book.
Limited User	Restricted from device management, all send functions and only allowed 2-sided printing and copying.
Guest	Restricted from device management, all send functions and only allowed 2-sided printing and copying.

The following functions and features can be restricted:

Gen 2		Gen 3 / DX	
Dep ID w/o AMS (with any Auth (DA, SSO-H or ULM))	Auth (SSO-H or ULM)	Auth (UA) w/o AMS Max 32 functions	Auth (UA or ULM) w/ AMS
MAX 3 functions	MAX 32 functions	MAX 32 functions	MAX 32 functions
Store/Access Files, Fax/i-Fax inbox	Copy	Copy	Copy
Send/Fax	Scan and Sent	Scan and Sent	Scan and Sent
Other	Fax	Fax	Fax
	Secured Print	Secured Print	Secured Print
	Access Store Files	Access Store Files	Access Store Files
	Scan and Store	Scan and Store	Scan and Store
	Fax/i-Fax Inbox	Fax/i-Fax Inbox	Fax/i-Fax Inbox
	Hold	Hold	Hold
	Scanner	Scanner	Scanner
	Printer	Printer	Printer
	Tutorial	Tutorial	Tutorial
	Web Access	Web Access	Web Access
	MEAP Applications	Dest./Fwd. Setting	Dest./Fwd. Setting
		Web Access favorite	Web Access favorite
		MEAP Applications	MEAP Applications

02

Device Security

When the Access Management System has been enabled, users must log in to the device using ULM, UA or SSO-H user authentication. Access Management System supports authentication through local device authentication as well as Active Directory using SSO-H, which includes support for Kerberos Authentication. Once a user logs into the device with their user name and password, 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 greyed out to the user after authentication.

Function Level Authentication

Canon imageRUNNER ADVANCE systems 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 colour or use the Scan and Send function.

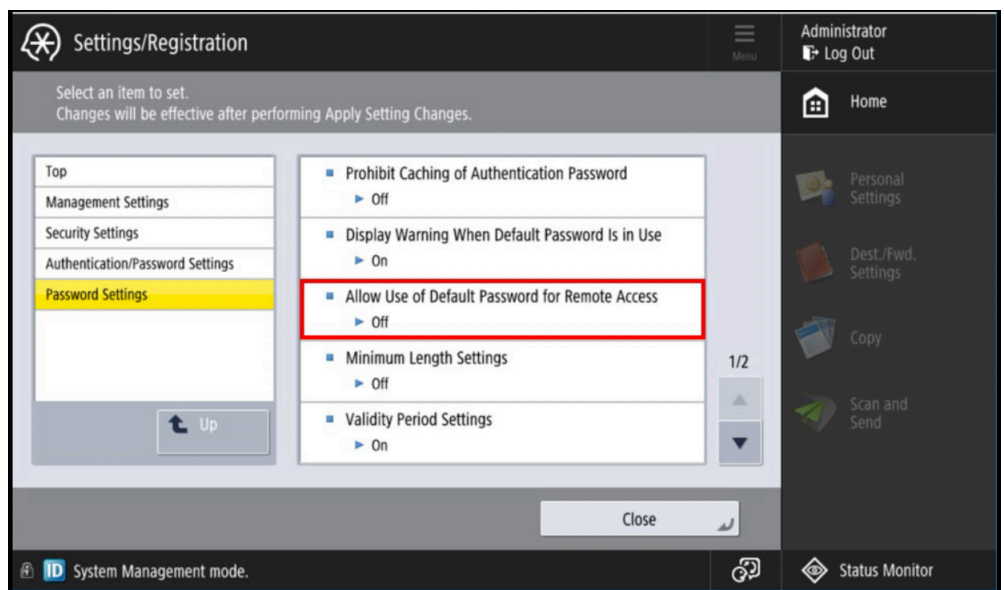
02 Device Security

Password-Protected System Settings

As a standard feature, imageRUNNER ADVANCE systems setup screens support password protection to restrict device setting changes from the control panel and Remote UI tool. System Administrators can set network information, system configuration, enable, and disable network and printing protocols among many other options. Canon highly recommends setting an administrator password at time of installation since it controls critical device settings.

Remote UI Default Password Change

To ensure good security practice, unique passwords should be used for each device or require the user to change the default password to a unique password before use. This prevents trivial remote access to the device until the default password/PIN for the Administrator/System Manager account is changed. This changes the ability to access the Remote UI through your web browser when the default password/PIN of “7654321” is currently set on the device. Depending on the series of device, access to the RUI will be prevented or the RUI will be disabled until the default password is changed.



02

Device Security

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, there are additional security features to prevent confidential information from being accessed.

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.

Access Code for Address Book

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.

Settings/Registration > Set Destination > Register Destinations > Register New Destinations, from here the user can register a new e-mail address, fax number, I-Fax, file or group address and set an access code for that specific address entry in the address book.

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 increases 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 [Favourite Settings] including destinations
- If you select [Send to Myself]

02 Device Security

SMB Protocol Support Chart (Send to SMB)

Series	SMB 1.0 supported	SMB 2.0 supported	SMB 3.0 supported	Special FW For SMB2.0/3.0
iR 1435 / 1435+ series	YES	YES	-	-
iR 1643 series	YES	YES	YES	-
iR 2500 series	YES	-	-	YES
iR 1700 series	YES	-	-	YES
iR ADV 400iF/500iF	YES	-	-	YES
iR ADV 3200 series	YES	-	-	YES
iR ADV 4000 series	YES	-	-	YES
iR ADV 4200 series	YES	-	-	YES
iR ADV 715iF II/III series	YES	YES	YES	-
iR ADV 4500/II/III series	YES	YES*	YES*	-
iR ADV DX 4700 series	YES	YES	YES	-
iR ADV 6000 series	YES	-	-	YES
iR ADV 6200 series	YES	-	-	YES
iR ADV 6500/II/III series	YES	YES*	YES*	-
iR ADV DX 6700 series	YES	YES	YES	-
iR ADV 8000 series	YES	-	-	YES
iR ADV 8200 series	YES	-	-	YES
iR ADV 8500/II/III series	YES	YES*	YES*	-
iR ADV DX 8700 series	YES	YES	YES	-
iR ADV C250iF/C350iF	YES	-	-	YES
iR ADV C255iF/C355iF	YES	YES*	YES*	-
iR ADV C256iF/II/III C356iF/II/III	YES	YES*	YES*	-
iR ADV C3300 series	YES	YES	-	YES
iR ADV C3500/II/III series	YES	YES*	YES*	-
iR ADV DX C3700 series	YES	YES	YES	-
iR ADV C5000 series	YES	-	-	YES
iR ADV C5200 series	YES	-	-	YES
iR ADV C5500/II/III series	YES	YES*	YES*	-
iR ADV C5700 series	YES	YES	YES	-
iR ADV C7000 series	YES	-	-	YES
iR ADV C7200 series	YES	-	-	YES
iR ADV C7500/II/III series	YES	YES*	YES*	-
iR ADV DX C7700 series	YES	YES	YES	-
iR ADV C475iF III series	YES	YES	YES	-
imagePRESS C165	YES	YES	YES	-

02

Device Security

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 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, 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 colour devices, watermarks and custom print profiles, as well as hiding any desired functions.

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.

Go to Settings / Registration > Preferences > External Interface > USB Settings.

All imageRUNNER ADVANCE models and select imageRUNNER models have the ability to restrict USB usage for memory, but allow USB usage for peripherals such as keyboards and card readers. Canon's USB feature provides the capability to view and print from the devices only for non-executable files, such as .pdf, .jpg, .tiff, and .png. Executable files cannot be performed on the device, and this prevents viruses from spreading if being accessed.

Third Party MEAP Application and Development

Canon actively collaborates with leading third-party software companies to develop custom solutions for imageRUNNER ADVANCE systems, known as MEAP applications. Each MEAP enabled device includes a number of safeguards to help ensure the security and integrity of information stored on the device.

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 an imageRUNNER ADVANCE system.

02

Device Security

Security Measures to Protect Against Malware and Tampering of Firmware/Applications

Since its inception, the imageRUNNER ADVANCE series has been designed with security in mind. Security measures to protect against malware/firmware tampering have been implemented that do not allow for installation or execution of programs without a digital signature applied by Canon when updating firmware, executing processes or installing MEAP applications. In order to further assist in the prevention of data disclosure due to unknown or springboard attacks, additional security enhancements have been made for the third generation imageRUNNER ADVANCE 3rd edition, imageRUNNER ADVANCE DX and imagePRESS C165.

The following program tampering detection function is introduced to counter unknown attacks:

- Verify System at Startup
- McAfee Embedded Control

Note: These features are only available on third generation imageRUNNER ADVANCE 3rd edition models, imageRUNNER ADVANCE DX and imagePRESS C165, and must be enabled. McAfee Embedded Control requires Unified Firmware Platform (UFP) v3.9 or later

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.

In order to use this function, the administrator should set "Verify System at Startup" to ON (Default: OFF).

- Settings/Registration > Management Settings > Security Settings > Verify System at Startup

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 or 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 and/or MEAP application.

02

Device Security

McAfee Embedded Control

Once enabled, McAfee Embedded Control allows only known programs contained in the dynamic whitelist to be executed on the MFD. Other programs not listed in the whitelist are considered unauthorized and will not be permitted to execute. This helps prevent worms, viruses, spyware, and other malware from compromising the device. A log of all prevented executions is available in the Audit Log when Runtime Intrusion Detection is enabled. McAfee Embedded Control delivers the following:

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

To turn on McAfee Embedded Control, it is necessary to turn on Verify System at Startup (Default OFF).

- Settings/Registration > Management Settings > Security Settings > Verify System at Startup

The administrator will also need to set "McAfee Embedded Control" to ON (Default OFF).

- Settings/Registration > Management Settings > Security Settings > McAfee Embedded Control

02

Device Security

Whitelists are created in each storage partition in which native device software modules are installed. McAfee Embedded Control checks the value held in the whitelist in advance of the module executing, and verifies the value generated by the execution of the module during operation. If the two values match, the verification is successful. If the two values do not match, the verification is unsuccessful, and execution of the module fails. The following outlines what will occur if the verification is unsuccessful:

- (a) The firmware verification process begins when the execution module registered in whitelist is started. If verification fails, the execution is blocked and an error code (E614-xxxx) is displayed.
- (b) When attempted execution of a non-registered software module is detected, the execution stops and the event is reported in the audit log.
- (c) When attempts to rewrite or delete a registered software module located on the whitelist is detected, the attempt is blocked and a record of the error code is saved in the audit log.
- (d) Validation of the whitelist itself is performed at startup of any software module. If tampering of the whitelist is detected, the execution is blocked and an error code is displayed. The error code is displayed according to the location of the software module where tampering was detected.
 - Error code example: (E614-xxxx for firmware, E602-xxxx for MEAP application)
- (e) The whitelist is updated as required when the system firmware is updated or when authorized MEAP applications are installed. In order to maintain consistency, when the software module is updated, the whitelist itself and the transaction log recording the change history of the whitelist are also updated.

Audit Log Related to Runtime System Protection Function

All recordable activities related to the Verify System at Startup and Runtime Intrusion Detection with McAfee Embedded Control processes are listed in the Device Management Log and can be notified in real time to a Security Admin through integration with a SIEM system.

03

Data Security

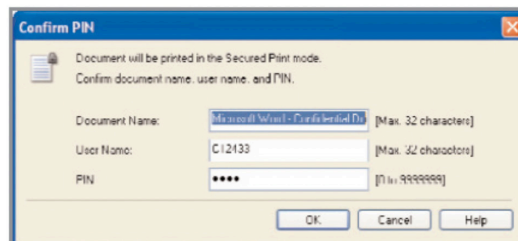
Protecting your organization's confidential information is a mission that Canon takes seriously. From your documents, faxes and e-mails to the underlying data on the internal hard disk drive and in memory, Canon has built in many controls to help ensure that your information does not become compromised.

Secure Printing

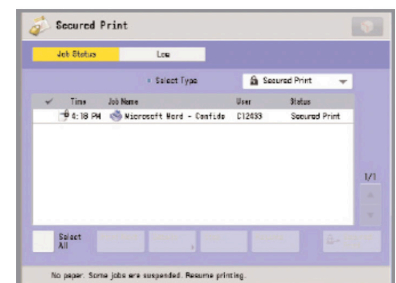
Secured Print / Encrypted Secured Print

Encrypted Secured Print and Secured Print are print functions that hold a job in queue until the user enters the appropriate password at the device. This ensures that the user is in close proximity before the document is printed and minimises unattended documents left at the device. The imageRUNNER ADVANCE system requires the user to set a password in the print driver window when sending a print job from a connected PC. The same password is also required for releasing the job at the device. When using the Encrypted Secured Print software*, security is further enhanced by using AES 256-Bit Encryption to protect the print job data while in transit across the network. On systems equipped with the optional Encrypted Secured Print, administrators can use the print job restriction feature to permit only encrypted print jobs at the designated device.

*the third Generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165 has this feature as standard.



Secured Print Screen from the Printer Driver



Print Job Status Screen

uniFLOW Secure Print

Exclusive to Canon is uniFLOW, which is optional modular software designed to reduce costs, improve productivity and enhance security. From a security perspective, uniFLOW provides secure printing capabilities by holding jobs at the server until released by the user at any desired imageRUNNER ADVANCE system. From their desktop, users print documents by choosing the uniFLOW server as the printer. At the chosen device, users can be authenticated using a wide variety of supported methods. If successful, access to the uniFLOW MEAP client application from the device's control panel is granted and the required job(s) can be selected and released from their queue of pending documents.

03

Data Security

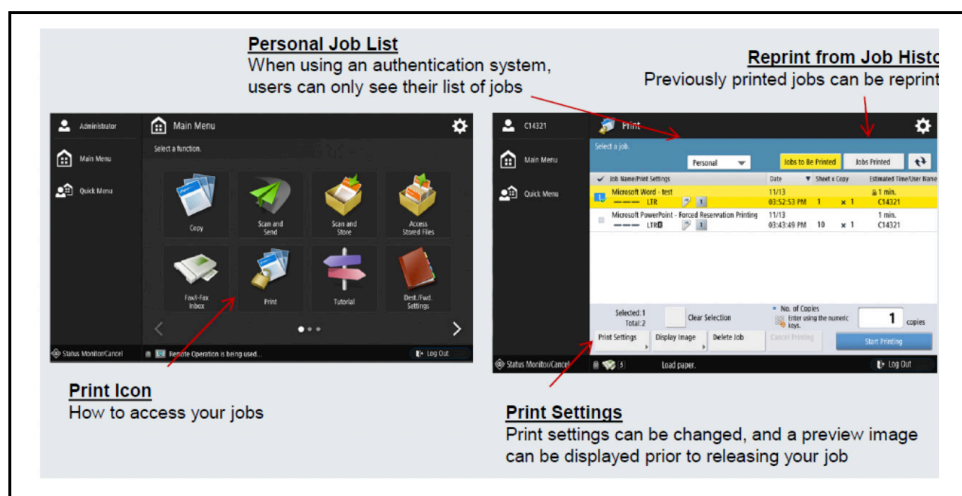
Forced Hold Printing

Canon third generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165 models come with an enhancement of the “Secure Printing” function, where IT administrators can enforce secure print for all, or select users. The setting only needs to be changed in the Settings/Registration screen on the local device UI. Print driver settings do not need to be changed.

Rules can be set up based on certain conditions (unknown owner, owner name, IP address, and/or port) to hold as a regular document, print immediately or cancel). Administrators can set how long documents in job hold will be held (from 10 min - 72 hours) and can choose whether to auto delete after printing or keep until expiration or manual deletion.

With Forced Hold 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 MFD.

Forced Hold Printing also helps to ensure that the user receives their desired output the first time, by allowing the user to preview their job, change print settings from the hold queue, and even print a sample file before printing an entire job.



03 Data Security

The chart below details the key differences between Forced Hold Printing, Secure Print, and Job Hold.

Supported Models	Gen2: N/A Gen3: All models imagePRESS Lite C165 DX: All models	Gen2: All models Gen3: All models imagePRESS C165 DX: All models	Gen2: iR-ADV 8200/ C7200/C9200 Series Gen3: iR-ADV 8500/6500/4500/ C7500/C5500 Series imagePRESS Lite C165 DX: iR-ADV DX 8700/6700/4700/ C7700 Series
Purpose of function	To prevent information leakage forcefully	To prevent information leakage on per job basis with user initiation	To print a trial before starting a large print job, print documents in the order of priority, or print after viewing the final settings
Set by	IT Manager	User	User
Set from	Settings/Registration, RUI	Print Driver	Settings/Registration to turn on [Hold] function Printer Driver (select "Hold")
Type of Setting	Per device	Per job	Per job
Access from	[Print] button	Gen2: [Secure Print] button Third Gen: [Print] button	[Hold] button
Authentication	With Auth, only your job is displayed in a personal job list	With Auth, only your job is displayed in a personal job list	N/A
Preview and Print / Change Settings	Yes (UFR II, PLC and PS)	Gen2: N/A Third Gen: YES (UFR, PCL and PS)	Yes
PIN input to print	N/A	Yes but can be skipped when authenticated	N/A
Job Capacity	Total 4GB, 2,000 files/per device, No per-user limit	Total 4GB, 2,000 files/per device, No per-user limit	BW model: 2,000 files CL model: 1,500 files (2,000 from Third Generation)
Job Storage Period *default	<10> (min.), <20> (min.), <30> (min.), *<1> (hr.), <2> (hr.), <3> (hr.), <6> (hr.), <12> (hr.), <1> (days), <2> (days), <3> (days)	<10> (min.), <20> (min.), <30> (min.), *<1> (hr.), <2> (hr.), <3> (hr.), <6> (hr.), <12> (hr.), <1> (days), <2> (days), <3> (days)	<0> (hr.), <1> (hr.), <2> (hr.), <3> (hr.), <6> (hr.), <12> (hr.), <1> (days), <2> (days), <3> (days), <7> (days), <30> (days)

- "Gen2" refers to Second Generation imageRUNNER ADVANCE C9200 Series, C7200 Series, C5200 Series C3300 Series, C2200 Series, C350iF/C250iF, 8200 Series, 6200 Series 4200 Series, 500iF/400iF
- "Gen3" refers to Third Generation imageRUNNER ADVANCE 8500 Series, 6500 Series, 4500 Series, C5500 Series, C7500 Series, C3500 Series, C355iF/C255iF, C356iF/C256iF
- "DX" refers to imageRUNNER ADVANCE DX 8700 Series, 6700 Series, 4700 Series, C7700 Series, C3700 Series

03

Data Security

Document Storage Space Protection

Mail Box Security

Each imageRUNNER ADVANCE system ships standard with Mail Boxes for storage of scanned and printed data. Mail Box security is provided by the ability to designate a unique password for access. Once a document is stored in the Mail Box (if the Mail Box is password protected), a user must enter their password to retrieve documents.

Advanced Box Security

The Advanced Box feature enables the imageRUNNER ADVANCE system to serve as a file sharing storage space. Users can save files in a shared folder, or within their own personal space in their native file format such as Word or PDF. Each user's personal space is protected with security credentials and requires the user to login prior to gaining access. Users can also store documents for others to access within the shared folder and any sub-folders.

Advanced Box also allows users to access their stored files from their desktop using Windows Explorer by mapping the folder as a network drive. Upon mapping or accessing the folder, the user will be prompted to authenticate through a Windows login box.

Administrators can manage the Advanced Box feature through the Remote UI interface and perform the following actions:

- Create user accounts and define type (Admin vs. End User)
- Activate authentication and enable Personal Space
- Register network devices for remote access
- Select the file formats allowed for storage (printable format only, common Office formats, or all).

By limiting to printable formats only, such as TIFF, JPEG and PDF, the risk of viruses that are commonly attached to .exe files is reduced. Also, the Advanced Box can be scanned by anti-virus software when shared as a network drive.

To prevent the storage of executable files that may contain viruses and other malicious code, system administrators can restrict the types of documents that can be saved to only printable formats, such as PDF, TIFF, and JPEG.

03

Data Security

Document Security Capabilities

Watermark / Secure Watermark

To discourage the unauthorized copying or sending of confidential information, imageRUNNER ADVANCE systems support the ability to embed user-defined text within the background of any print or copy job. When duplicates are made by photocopying, the secure watermark appears. Secure Watermark feature can be set for all print jobs or assigned by the user through the print driver. Users can also define custom or pre-set watermarks to appear in any position on copied output.

Encrypted PDF

The Encrypted PDF mode 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.

Encrypted PDF mode can be used only if an e-mail address or file server is specified as the destination. If a fax number, I-fax address, or inbox is specified as the destination, a user cannot send the job as an encrypted PDF file. Encrypted PDF files can be saved using 40bit RC4, 128bit RC4 or the 128bit AES algorithms. When sending with Encrypted PDF 128bit AES, Acrobat 7.0 or later is required to open the PDF file. With the imageRUNNER ADVANCE devices Encrypted PDF offers AES 256-bit support.

*Encrypted PDF is standard on 2nd edition, 3rd edition, imageRUNNER ADVANCE DX and imagePRESS C165

03

Data Security

Digital Signature PDF (Device and User Signature)

Within Scan and 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.

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.

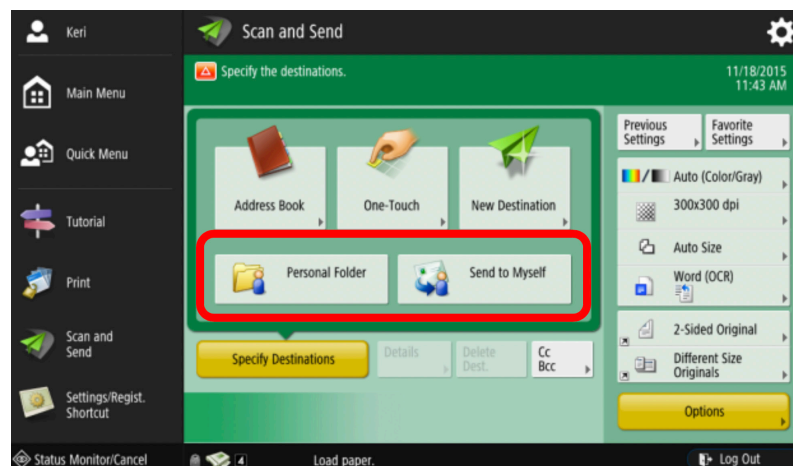
Canon imageRUNNER ADVANCE systems also support a feature called PDF Visible Digital Signature, which forces the display of the digital signature on the first page of the PDF file rather than recipients having to open the document's properties. Users can select the visible signature from the Scan and Send screen. This not only makes the digital signature more prominent, but also ensures that the digital signature appears on any printed versions of the document.

*Device Signature is standard on 2nd edition

Send to Myself (only)

Another feature in the imageRUNNER ADVANCE series applies to document distribution solutions, called Send to Myself (only). This new feature allows administrators to configure the device so that users are only able to Scan and Send documents to their own e-mail or personal folder. This document distribution security feature prevents information leakage by disallowing walk-up users to type in just any email address to send scanned documents.

* "Folder and E-mail information have to be registered in user account in authentication system.



03

Data Security

Copy Set Numbering

All imageRUNNER ADVANCE systems support the ability to add copy set numbers to copied and printed output in a user-defined region on the page. Copy set numbering offers a means to track documents by the set number that a recipient receives.

A wide variety of device and network security features are standard on imageRUNNER ADVANCE systems. Canon recognizes that each customer's needs are different, therefore Canon offers various advanced security options to assist companies in meeting their internal privacy goals and address regulatory guidelines that may be applicable to certain environments.

These options have been developed in accordance with the extended security requests of key customers and government agencies. Canon offers advanced security features that protect data stored on the device and during transmission.

Data Storage

HDD and RAM Data Protection

All imageRUNNER ADVANCE systems require hard disk and RAM for their normal operation. The partitions on the imageRUNNER ADVANCE hard disk are formatted with one of the following types of file systems:

- iR File System
- FAT 32-Compatible File System

The "iR File System" is a Canon proprietary file system that was designed solely for the processing of image files in a fast and efficient manner. This file system is not compatible with commonly used PC file systems, and therefore analysing its data at the sector level is extremely difficult.

The "FAT32 Compatible File-System" is the file system used by the imageRUNNER ADVANCE for the disk areas that store the system firmware, MEAP applications, Mail Box and Advance Box files.

In general, it is difficult to analyse the data on these file systems at the sector level, however, Canon recognizes that highly motivated and experienced attackers may try to obtain information from environments where sensitive information is processed, by analysing the hard disks from these devices. In order to help protect your sensitive and confidential information Canon imageRUNNER ADVANCE systems include a standard hard disk format utility, as well as more advanced optional accessories, such as the HDD Data Erase Kit and/or HDD Data Encryption Kit. With the second and third generation imageRUNNER ADVANCE devices, HDD Data Erase comes as standard.

* Some imageRUNNER ADVANCE systems that are configured with the optional HDD Mirroring Kit for external Print Controller may contain more than one disk

03

Data Security

Standard HDD Initialize

Best practices, and often company policies, usually recommend that systems be completely wiped by the system administrator prior to the device being reallocated to a new location or prior to the end of lease or at the end of its lease. The Hard Disk Drive Initialize feature, which is standard on all imageRUNNER ADVANCE systems, overwrites all user data areas on the hard disk.

Overwrite mode supported for the HDD Initialize function include:

- Overwrite once with null (default)
- Overwrite once with random data
- Overwrite three times with random data
- Overwrite three times in the following order (DoD Standard):
 - Fixed value
 - Complement number of fixed value
 - Random data
- Overwrite nine times with random data

Overwritten information includes:

- Data stored in Mail Boxes and Advanced Box
- Data stored in Fax/I-Fax Inbox (Confidential Fax Inbox/Memory RX Inbox)
- Address data stored in the Address Book
- Scan settings registered for the Sending function
- Mode Memory settings registered for the Copy or Mail Box function
- MEAP applications
- Data saved from MEAP applications
- The password for the SMS (Service Management Service) login service of MEAP
- User authentication information registered in the Local Device Authentication system of UA or SSO-H (Single Sign-On H)
- Unsent documents (reserved documents and documents set with the Delayed Send mode)
- Job history
- Settings/Registration settings
- Forms registered for the Superimpose Image mode
- Registered forwarding settings
- Key Pair and Server Certificate registered in [Certificate Settings] in [Device Management] in Management Settings (from the Settings/Registration screen)

After the HDD Initialize the device will print a report with device serial number, device name, erase mode, date and time of erasing, firmware version.

03

Data Security

HDD Data Encryption Function

The HDD Data Encryption Kit (standard on third generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165 devices), which has achieved Common Criteria Certification of Evaluation Assurance Level 2 (EAL2), ensures that all data stored on the internal disk drive is protected using industry-standard algorithms. The HDD Data Encryption Kit for imageRUNNER ADVANCE systems uses a dedicated plug-in board that encrypts every byte of data before it is committed to the disk using the 256-bit AES (Advanced Encryption Standard) algorithm. The HDD Encryption chip has been updated to obtain FIPS 140-2 validation (only for Third Generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165)

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB140-2), is a U.S. government computer security standard used to accredit cryptographic modules.

The title is Security Requirements for Cryptographic Modules.

FIPS 140-2 Validation

imageRUNNER ADVANCE (Gen2/3), imageRUNNER ADVANCE DX and imagePRESS C165 have cryptographic modules accredited by FIPS140-2 certification (level 1).

The following functions conform to FIPS140-2 using the cryptographic modules.

<Gen2/3>

- IPsec

<Gen3 Only>

- TLS
- MEAP application (MEAP application implemented to use FIPS provider only)
- HDD encryption chip

Though IPsec always operated in the FIPS mode on third generation imageRUNNER ADVANCE, imageRUNNER ADVANCE DX and imagePRESS C165 devices, a setting must be specified from the UI screen or the Remote UI for TLS to format encryption method and MEAP to FIPS 140-2.

03 Data Security

Additional Secure Cipher Algorithms Supported

Encryption algorithms have been added to encryption modules used by MEAP applications (Java Cryptography Extension : JCE). Expanding the encryption algorithms used by MEAP applications enables the machine to support requests for a wider range of encryption algorithms.

	Conventional Encryption Algorithms	FIPS Encryption Algorithms
Message digest	MD4, MD5, SHA-1, SHA-224/256/384/512	SHA-1, SHA-224/256/384/512
Message authentication code	HMAC-MD5, HMAC-SHA1, HMAC-SHA224, 356, 384, 512	HMAC-SHA1, HMAC-SHA224, 356, 384, 512
Common key encryption	DES, 3DES, RC4, AES (CBC,CFB,CTS, GCM)	3DES, AES (CBC,CFB, GCM)
Public key encryption	RSA	RSA (2048 bit -)
Key pair generation	RSA, ECDSA, DSA	RSA (2048 bit -), ECDSA, DSA (2048 bit -)
Common key generation	PBKDF2 With HmacSHA1 PBKDF2 With HmacSHA224 PBKDF2 With HmacSHA256 PBKDF2 With HmacSHA384 PBKDF2 With HmacSHA512	PBKDF2 With HmacSHA1 PBKDF2 With HmacSHA224 PBKDF2 With HmacSHA256 PBKDF2 With HmacSHA384 PBKDF2 With HmacSHA512
Key sharing	ECDH, DH	ECDH DH (2048 bit -)
Random number generation	DSASHA/DSADES	DSASHA/DSADES
Digital signing	SHA1/MD2/MD5/SHA224/SHA256/SHA384/SHA512 with RSA SHA1 with DSA SHA1/SHA224/SHA256/SHA384/SHA512/ with ECDSA	SHA1/SHA224/SHA256/SHA384/SHA512 with RSA SHA1 with DSA SHA1/SHA224/SHA256/SHA384/SHA512/ with ECDSA
Key pair, format	PKCS#12	PKCS#12

03

Data Security

HDD Data Erase Function

The HDD Data Erase Kit (now standard on second and third generation imageRUNNER ADVANCE models, imageRUNNER ADVANCE DX and imagePRESS C165) enables system administrators to configure their imageRUNNER ADVANCE to overwrite the internal image server hard disk and erase previous data as part of routine job processing. The technology can be set to overwrite:

1. Once with null data,
2. Once with random data,
3. Three times with random data,
4. Overwrite three times in the following order (DoD Standard - DoD 5220.22-M compliant):
 - a. Fixed value
 - b. Complement number of fixed value
 - c. Random data

Standard DoD 5220.22-M is a data clearing and sanitizing method used to overwrite existing information on a hard drive. This method will prevent all software and hardware based file recovery methods from lifting information from the hard drive.

HDD Data Erase Scheduler MEAP

The optional HDD Data Erase Scheduler MEAP application adds more functionality to the existing HDD overwriting functions allowing administrators to now schedule when to overwrite the Canon device's HDD. Additionally, the HDD Data Erase Scheduler generates a printed confirmation report upon completion of the HDD data erase. This MEAP application meets the customer requirements for easier and more automated HDD erasing and the need for a printed confirmation that this important security function has been executed.

Key features include:

- Set daily, weekly and monthly schedule for overwriting HDD data
- Overwrite HDD data on-demand by the push of a button
- Receive a printed or emailed confirmation report upon execution of scheduled or on-demand overwriting

The HDD Data Erase Scheduler will overwrite up to 3 times, depending on how the HDD Data Erase Function is activated on the device. Users can select the overwrite mode in the device settings.

03

Data Security

Removable HDD Kit

The imageRUNNER Removable HDD Data Kit option (no longer available) provides a means for system administrators to physically lock the device's internal hard disk drive into the system during normal operation, thereby decreasing the risk of theft. Once the device has been powered down, the drive can be unlocked and removed for storage in a secure location. There is no Removable HDD Kit option for DX models, but DX models (excluding C3700 Series) can have their HDD removed. When the connector reaches its service life, it must be purchased and replaced by a service technician. Parts are as follows:

Model	Part Number
iR-ADV DX C3500	FK4-4075
iR-ADV DX C7700	FK4-2497
iR-ADV DX 4700	FK4-6476
iR-ADV DX 6700	FK4-2497
iR-ADV DX 8700	FK4-2497

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. The administrator can select [On] or [Off] for Job Log Conceal under Settings / Registration > Management Settings > Device Management > Display Log.

When [On] is selected, the job log is displayed. If Job Log Display is set to [Off], the following features and settings will not be displayed on screen or activated:

- Copy, send, fax, and, print log from System Monitor
- Receive from system monitor Send Activity management report when equipped with Canon's optional Scan and Send Kit.
- Fax Activity management report
- Auto print is set to [Off] disabling the Daily Send & Fax Activity Report

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

03

Data Security

Trusted Platform Module (TPM)

Every imageRUNNER ADVANCE system includes a Trusted Platform Module (TPM), a tamper-resistant open standards security chip that is responsible for encrypting and decrypting information such as passwords, certificates, IDs and cryptographic keys. TPM protects information on the internal hard disk drive by storing the encryption key in a separate location. Once enabled, the device will not launch if the TPM chip is removed to protect against physical attacks.

TPM functionality is disabled by default. The feature can be enabled on Canon imageRUNNER ADVANCE devices within the Additional Functions menu. Once enabled, it is important to back up the TPM key in the event of failure through USB memory which must be then stored in a safe and secure location.

HDD Password Lock

The imageRUNNER ADVANCE Series offer a feature called HDD Lock. HDD Lock provides the capability of securing the HDD with a Password making it difficult to access the data that is stored on the hard disk to be accessed. If the HDD is physically removed from the device, its data cannot be accessed via a PC. This feature does not encrypt the hard drive.

Data in Transit

Encrypted PDF

The Encrypted PDF feature of imageRUNNER ADVANCE systems support 40-bit/128-bit RC4 encryption and 128-bit AES (Advanced Encryption Standard) for greater security when sending documents. When sending a 128-bit AES encrypted PDF, Acrobat 7.0 or later is required to open the file. For the imageRUNNER ADVANCE devices, 256-Bit AES encrypted PDF is supported.

For more information, please refer to the Document Security section, under Information Security.

03

Data Security

Fax Security

Super G3 Fax Board and Multi Line Fax Board

Canon imageRUNNER ADVANCE systems that support Super G3 fax capabilities with the optional Super G3 Fax Board installed can be connected to the Public Switched Telephone Network for sending and receiving of fax data. In order to maintain the security of customer's networks in relation to this potential interface, Canon has designed its Super G3 Fax Boards to function in accordance with the following security considerations:

Super G3 Fax Board Communication Mechanism

The modem on the Super G3 Fax Boards does not have Data Modem capability, but only Fax Modem capability. As a result, TCP/IP communication through the phone line is impossible. In addition, there is no functional module such as a Remote Access Service that enables communication between a phone line and a network connection within the device.

Fax Transmission

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.

Fax Received

Although a received fax document can be accessed from the network through the Confidential Fax Mail Box function inherent in the device or automatically forwarded to a network, it is not possible to breach the network in either instance as these capabilities are afforded following completion of facsimile communication. Since the data stored in the Confidential Fax Mail Box is in a format proprietary to Canon, there is no threat of virus infection. Even if the device receives a data file pretending to be a FAX image data but contains a virus, the received data must be decoded first. While trying to decode the virus the phone line will be disconnected with a decode error and the received data will be discarded. The Super G3 Fax Boards cannot receive data files, they are only capable of receiving and decoding facsimile transmissions. As a result, virus-laden files sent to an imageRUNNER ADVANCE system via its phone line connection cannot be processed.

Other Fax Features

Allow/Restrict Fax Driver Transmissions

Device can be configured to allow (default) or restrict sending fax transmissions via a PC Fax driver. To set this function, go to: [Function Settings][Send][Fax Settings][Allow Fax Driver TX]

Allow/Restrict Sending from History (Job Log)

The device can be configured to allow (default) or restrict recalling the last three addresses, scan settings, or send settings used, for sending.

To set this function, go to: [Function Settings] [Send][Common Settings][Restrict Resending from Log] ON: Prohibit fax redialling OFF: Allow fax redialling (Default)

Fax Forwarding / Mailbox Fax Forwarding

The Fax Forwarding function allows imageRUNNER ADVANCE systems equipped with a fax board to forward inbound fax transmissions to specific recipients. This is done by setting predetermined conditions or storing faxes in a secure Memory Reception Inbox for later printing rather than permitting incoming messages to pile up in an open output tray.

Advanced Box Fax Forwarding & Fax Received Notification

Similar to the Fax Forwarding function, imageRUNNER ADVANCE systems support 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 Advanced Box location, 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.

Fax Destination Confirmation

To help prevent faxed documents from being inadvertently sent to the wrong destination, imageRUNNER ADVANCE systems offer a 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.

Fax Storage Space

Fax Mail Box and Advanced Box Fax Security

Incoming faxes on imageRUNNER ADVANCE systems can be automatically routed to a designated Mail Box or Advanced Box, which can be password-protected to prevent the contents from being viewed by unauthorized individuals.

04

Network Security

Network and Print Security

Canon imageRUNNER ADVANCE systems include a number of configurable network security features that assist in securing information when networking printing is installed. Standard network security features include the ability to permit only authorized users and groups to access and print to the device, limiting device communications to designated IP/MAC addresses, and controlling the availability of individual network protocols and ports as desired.

Enabling/Disabling Protocols/Applications

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. Canon imageRUNNER ADVANCE systems have the ability to disable unused TCP/IP ports to further secure the devices. Disabling ports affects the available functions and applications on the device. Configurable ports* include:

imageRUNNER ADVANCE Port Summary (see next page)

04 Network Security

imageRUNNER ADVANCE Port Summary

Name	Port	Default	Description	Setting
TCP				
LPD LPD	515	ON	LPD print	[Preferences]->[Network]->[TCP/IP Settings]->[LPD Print Settings]
RAW	9100	ON	RAW print	[Preferences]->[Network]->[TCP/IP Settings]->[RAW Print Settings]
HTTP	80	ON	World Wide Web HTTP	[Preferences]->[Network]->[TCP/IP Settings]->[Use HTTP]
HTTPS	443	OFF	HTTP over TLS/SSL	[Preferences]->[Network]->[TCP/IP Settings]->[Confirm Dept. ID PIN] [Preferences]->[Network]->[TCP/IP Settings]->[IPP Print Settings]->[Use SSL] [Set Destination]->[Make Remote Add. Book Open]->[Make Address Book Open] [Management Settings]->[Device Settings]->[Device Information Delivery Settings]->[Restrict Receiving for Each Function] [Function Settings]->[Send]->[E-Mail/1-FAX Settings]->[Communication Settings]->[Authent./Encryption]->[Allow SSL(SMTP Receive)]
HTTP (MEAP)	8000	ON	World Wide Web HTTP for MEAP	[Preferences]->[Network]->[TCP/IP Settings]->[Use HTTP]
HTTPS (MEAP)	8443	OFF (*1), ON (*2)	World Wide Web HTTP for MEAP	[System Settings] -> [MEAP Settings] -> [Use SSL]
SMTP	25	OFF	Simple Mail Transfer Protocol	[Function Settings] -> [Send] -> [E-mail/1-Fax Settings] -> [Communication Settings] -> [SMTP RX] COPIER>OPTION>Network> SMTPRXPN COPIER>OPTION>Network> SMTPTXPN
IPP	631	OFF	Internet Printing Protocol	[Preferences]->[Network]->[TCP/IP Settings]->[IPP Print Settings]
FTP	21	OFF	File Transfer Protocol	[Preferences]->[Network]->[TCP/IP Settings]->[FTP Print Settings]->[Use FTP Printing]
netbios-ssn	139	OFF	NETBIOS Session Service (SMB)	[Preferences]->[Network]->[SMB Server Settings]->[Use SMB Server]
CIFS	445	OFF	CIFS	[Preferences]->[Network]->[SMB Server Settings]->[Use SMB Server]
VNC	5900	OFF	Canon VNC port	[Management Setting]>[License/Other]>[Remote Operation Setting]
SSO-H	0000-1010	OFF	Single Sign-On Hybrid (Only when SSO-H Login Service is selected)	[SMS]System Management>Enhanced Sys. App
RemoteConsole	19001	OFF	JVM RemoteConsole (Debug for MEAP Application)	[MEAP Developer's Dialog]Remote Console Functions
Remote Fax	20317	OFF	Remote Fax	[Function Settings]->[Send]->[FAX Settings]->[Remote FAX Settings]->[Use Remote FAX]
WSDScan	60000	OFF	WSDScan	[Preferences]->[Network]->[TCP/IP Settings]->[WSD Settings]->[Use WSD Scan Func]
SIP	5060	OFF	IP FAX	[Preferences]->[Network]->[TCP/IP Settings]->[SIP Settings]
SIP REGIST (TLS)	5061	OFF	IP FAX	-
t38	49152	OFF	IP FAX	[Preferences]->[Network]->[TCP/IP Settings]->[SIP Settings]
UDP				
SNMP	161	ON	SNMP	[Preferences]->[Network]->[SNMP Settings]->[Use SNMPv.1] [Preferences]->[Network]->[SNMP Settings]->[Use SNMPv.3]
SLP	427	OFF	Service Location Protocol	[Preferences]->[Network]->[TCP/IP Settings]->[Multicast Discovery Settings]->[Response]
WSD	3702	OFF	WSD WS-Discovery	[Preferences]->[Network]->[TCP/IP Settings]->[WSD Print Settings]->[Use WSD]
IPsec	500	OFF	IPsec IKEv1	[Preferences]->[Network]->[TCP/IP Settings]->[IPsec Settings]->[Use IPsec]
IPsec	4500	OFF	IPsec IKEv1	[Preferences]->[Network]->[TCP/IP Settings]->[IPsec Settings]->[Use IPsec]
BMLinkS	1900	OFF	BMLinkS Discovery	[Preferences]->[Network]->[TCP/IP Settings]->[BMLinkS Settings]->[Use BMLinkS]
mDNS	5355	OFF	mDNS / mDNS-SD	[Preferences]->[Network]->[DNS Settings]->[mDNS Settings]->[Use mDNS IPv4] [Preferences]->[Network]->[DNS Settings]->[mDNS Settings]->[Use mDNS IPv6]
SIP	5060	OFF	IP FAX	[Preferences]->[Network]->[TCP/IP Settings]->[SIP Settings]
RTP	5004	OFF	IP FAX	[Preferences]->[Network]->[TCP/IP Settings]->[SIP Settings]
RTCP	RTP+1(5005)	OFF	IP FAX	-
t38	49152	OFF	IP FAX	[Preferences]->[Network]->[TCP/IP Settings]->[SIP Settings]
The port opened only while transmitting data.				
airfax event	29400	-	AIR FAX Event	Just while AIRFax is sending
smb	31050-79	-	SMB Printing Data	Just while SMB is printing
SSO-H	1-65535	-	Single Sign-On Hybrid (Only when SSO-H Login Service is selected Authentication data sending)*	[SMS]System Management>Enhanced Sys. App
DIS	1025-65535	-	DSL Installer Service (Communicate with ESM)	MEAP Enterprise Service Manager

04 Network Security

IP Address Filtering

The imageRUNNER ADVANCE Series support two types of IP Address Filtering as described below. Third Generation allows for the choice between Type1 and Type2 .Second Generation only allows for “IP Address Filtering Type 2(Receiving and Transmitting Packets)”.

- **IP Address Filtering Type1 (Receiving Packets)**

IP Address Filtering Type 1 is a function to permit or reject reception of packets from the specified IP Addresses. Administrators can decide to enable IP Filtering for the RX Print and Setting/Browsing functions, and can specify filtering options (Permit/Reject).

Up to eight individual IP addresses or IP address ranges can be specified. The default value of all options for this feature is “Disable” (permit reception).

The target applications (protocols) and the number of addresses that may be specified are as follows:

Category	Conventional Encryption Algorithms	FIPS Encryption Algorithms	
RX Print	Permit	IPv4 : 8, IPv6 : 8	LPD, RAW, SMB, FTP HTTP (IPP), PDF, SMTP, BMLinks, WSD
	Reject	IPv4 : 8, IPv6 : 8	
Setting/Browsing	Permit	IPv4 : 8, IPv6 : 8	SNMP, HTTP (RUI), SLP
	Reject	IPv4 : 8, IPv6 : 8	

- **IP Address Filtering Type 2 (Receiving and Transmitting Packets)**

IP Address Filtering Type 2 is a function to permit or reject reception (RX) and transmission (TX) of packets to and from the specified IP Addresses. There is no distinction between “RX/Print” and “Setting/Browsing” as there is with IP Address Filtering Type 1.

A maximum of 16 addresses may be registered for RX packets and TX packets, respectively. Note that IPv4 addresses and IPv6 addresses are registered separately.

The previous distinction between “RX/Print” and “Setting/Browsing” no longer exists.

The setup required for filtering involves configuration of the default policy (either Reject or Permit), followed by registration of the IP addresses to be exempt.

04

Network Security

If the default policy is to “Permit,” then the IP addresses you want to reject must be registered. Conversely, if the default policy is to “Reject,” then the IP addresses you want to permit must be registered. The default value for the default policy is to “Permit” for both reception and transmission.

- Port Number Blocking Function

This function controls (rejects or permits) data reception for the specified port number.

Since port numbers can also be specified for the IP Address Filtering Function, the default policy is subordinate to the IP Address Filtering Function.

In other words, if the default policy is to permit, then port numbers to reject should be specified, and if the default policy is to reject, then the port numbers to permit should be specified.

Initial value for the default policy is “Permit”.

Remote UI Login Time Out Period Setting

Only available on Third Generation, imageRUNNER ADVANCE DX series and imagePRESS C165.
Requires Unified Firmware Platform (UFP) v3.10

This function gives some flexibility for users to set time out period for remote login. Previously Time out period setting after logging in to Remote UI was fixed at 15 minutes. With this function, setting value can be set from 15min to 150min. (Default settings: 15min)

[Settings/Registration] > [Preferences] > [Network Settings] > [Session Settings] > [Timeout After Logging in to Remote UI] *This can be set up only from RUI (not supported from local UI)

Media Access Control (MAC) Filtering

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.

Up to 100 MAC addresses can be registered and easily added, edited, or deleted through the Remote UI interface. MAC address filters take a higher priority than the IP address filters; so necessary systems can be allowed or denied, even if the system's IP address would dictate otherwise. The imageRUNNER ADVANCE Series support two types MAC address filtering: Type 1 filters received packets (RX) and Type 2 filters received (TX) and transmitted packets (TX).

04 Network Security

SSL/TLS Encryption

Many organizations are quite diligent about protecting data as it is transferred between PCs and servers or from one PC to another. However, when it comes to transmitting that same data to and from the MFD device, it is almost always sent in clear text. As a result, it may be possible to capture all the data as it is sent to the printer via the network. Canon helps mitigate this dilemma by providing Secure Socket Layer (SSL 3.0) encryption and Transport Layer Security (TLS 1.0/1.1/1.2) (for support of some transmissions to and from the imageRUNNER ADVANCE device, such as Internet protocol Printing (IPP), Internet-fax (I-fax), Remote UI, Web Access and DIDF.

The imageRUNNER ADVANCE series supports Transport Layer Security, which is a connection-type transport layer protocol for HTTP security. It provides authentication and encryption, as well as detects alternations. Common practice is that a TLS server submits CA certificates with specific expiration dates while a client verifies its authenticity.

	First Generation iR ADVANCE C9000 Series, C7000 Series, C5000 Series, C2000 Series, 4000 Series, 6000 Series, 8000 Series,	Second Generation iR ADVANCE C9200 Series, C7200 Series, C5200 Series, C3300 Series, C2200 Series, C350iF/C250iF, 8200 Series, 6200 Series, 4200 Series, 500iF/400iF	Third Generation iR ADVANCE 8500 Series, 6500 Series, 4500 Series, C5500 Series, C7500 Series, C3500 Series, C355iF/C255iF, C356iF/C256iF 715iF Series/C475iF Series imagePRESS C165	iR ADVANCE DX 8700 Series, 6700 Series, 4700 Series, C7700 Series, C3700 Series
SSL 3.0	Supported	Supported	Not Supported	Not Supported
TLS 1.0	Supported	Supported	Supported	Supported
TLS 1.1/1.2	Supported	Supported	Supported	Supported
TLS 1.3	Not Supported	Not Supported	Supported	Supported

04 Network Security

TLS Version Selection

Only available on Third Generation, imageRUNNER ADVANCE DX series and imagePRESS C165.
Requires Unified Firmware Platform (UFP) v3.10

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. TLS 1.3 can be set on Gen3 3rd Edition, DX series and imagePRESS C165 (Unified Firmware Platform V3.10 required). If a vulnerability is discovered in an old version(s) of TLS, the administrator can disable that version in the device to help maintain security.

Note: When TLS1.3 is set, it may be unable to communicate depending on the destination's version. For example, some web browsers version do not support TLS 1.3. Therefore, if the upper limit and lower limit of TLS versions are both set to TLS1.3, these browsers fail to access to the device with TLS. Also, TLS 1.3 may not be supported with some MEAP applications, including uniFLOW.

To modify TLS versions, go to: Preferences > Network > TCP/IP Settings > TLS Settings > Specify Allowed Versions



Communication fails if the MEAP app communication server does not support the TLS version specified with “Settings/Registration”.

04 Network Security

Cipher Algorithm Selection (Including disabling 3DES)

(Only available on Third Generation)

The administrator can strengthen security by adapting IPSec and TLS encryption algorithms to their operation policy. Cypher algorithm selection enables the selection of encryption algorithms/signing algorithms for TLS communication. This setting has been added for restricting AES-CBC/GCM key lengths to 256 bit when using IPSec. Previously, 128 bit/256 bit could be selected together, but now security can be enhanced by restricting to 256 bit only.

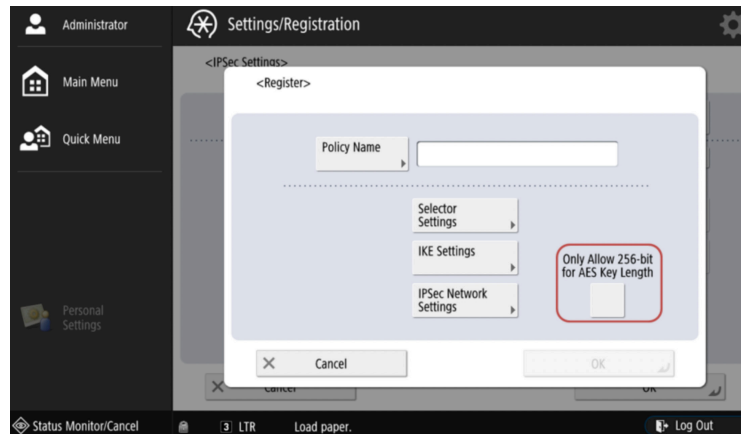
User mode settings allows to select cipher suites to be used. The administrator can put it together with a choice of TLS version, encryption algorithm, key distribution algorithm, signature algorithm and HMAC algorithm. In this way, it prevents the algorithm that users do not want to use from being chosen it.. (If the combination of version and algorithm cannot be used, the error screen pops up when pressing “OK”)

Version	Encryption Algorithm	Key Exchange Algorithm	Signature Algorithm	HMAC Algorithm
TLS 1.0	AES CBC (256 bit)	RSA	RSA	SHA 1
TLS 1.1	AES GCM (256 bit)	ECDHE	ECDSA	SHA 256
TLS 1.2	3DES CBC	X25519 (*1)		SHA 384
TLS 1.3	AES CBC (128 bit)			
	AES GCM (128)			
	CHACHA20_ POLY1305 (*1)			

(*1): Selectable only with TLS1.3

Flow of IPSec Settings

An “Only Allow 256-bit for AES Key Length” button has been added to the IPSec policy settings screen (Preferences > Network > TCP/IP Settings > IPSec Settings).

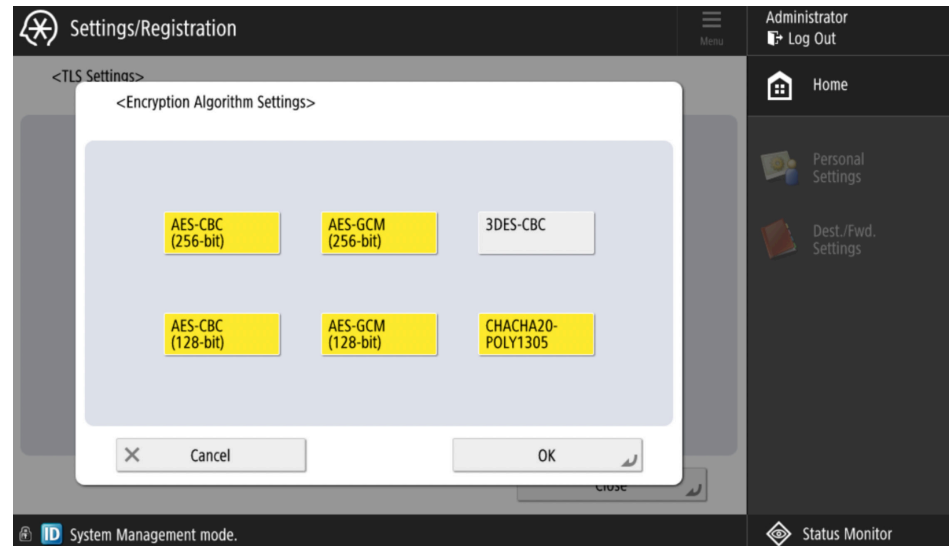


04

Network Security

Flow of TLS Settings

Encryption/signing algorithms can be selected on the TLS algorithm settings screen (Preferences > Network > TCP/IP Settings > TLS Settings).



IPv6 Support

IPv6 support, which is available in all imageRUNNER ADVANCE systems, provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4.

IPSec Support

Canon imageRUNNER ADVANCE systems support IPSec, which allows users to utilize IPSec (Internet Protocol Security) to help ensure the privacy and security of information sent to and from the device, while in transit over unsecured networks. With the imageRUNNER ADVANCE devices, IPSec Support is standard, and it is built directly into the firmware and no optional “Boards” are required.

IPSec is a suite of protocols for securing IP communications. IPSec supports secure exchange of packets at the IP layer, where the packets in the data stream are authenticated and encrypted. It encrypts traffic so that the traffic cannot be read by parties other than those for whom it is intended, it also ensures that the traffic has not been modified along its path and is from a trusted party, and protects against replay of the secure session. The IPSec functionality of the device only supports transport mode, therefore authentication and encryption is only applied to the data part of the IP packets.

04

Network Security

Authentication and Encryption Method:

One of the following methods must be set for the device.

- AH (Authentication Header)

A protocol for certifying authentication by detecting modifications to the communicated data, including the IP header. The communicated data is not encrypted.

- ESP (Encapsulating Security Payload)

A protocol that provides confidentiality via encryption while certifying the integrity and authentication of only the payload part of communicated data.

Key Exchange Protocol

Supports IKEv1 (Internet Key Exchange version 1) for exchanging keys based on ISAKMP (Internet Security Association and Key Management Protocol). IKE includes two phases; in phase 1 the SA used for IKE (IKE SA) is created, and in phase 2 the SA used for IPSec (IPSec SA) is created.

To set authentication with the pre-shared key method, it is necessary to decide upon a pre-shared key in advance, which is a keyword (24 characters or less) used for both devices to send and receive data. Use the control panel of the device to set the same pre-shared key as the destination to perform IPSec communications with, and perform authentication with the pre-shared key method.

To select authentication with the digital signature method, it is necessary to install a key pair file and CA certificate file created on a PC in advance using the Remote UI, and then register the installed files using the control panel of the device. Authentication is conducted with the destinations for IPSec communication using the CA certificate.

The types of key pair and CA certificate that can be used for authentication with the digital signature method are indicated below.

- RSA and ECDSA algorithm
- X.509 certificate
- PKCS#12 format key pair

04

Network Security

FTPS Support

Only available on Third Generation and imageRUNNER ADVANCE DX series and imagePRESS C165. Requires Unified Firmware Platform (UFP) v3.10

Canon imageRUNNER ADVANCE series support the FTPS function defined in RFC2228 and RFC4217 using TLS for additional security on FTP send function. Executes TLS communication when FTPS is specified as the send destination, and ends with error code #801 if TLS communication fails. It enables users to securely use by encrypting FTP communication.

FTPS can be used by using “ftps://host name/” when TLS is enabled on entering the host name of the file server/Advanced Box which transmits data.

Network Authentication

Authentication mechanism used by the network applications and their support statuses are described below.

	Plain	CRAM-MD5	LM	NTLM	NTLMv2	Kerberos
IFAX/SMTP AUTH	o (Plain/Login)	o	x	o	x	o
SMB Send/Browse	x	x	o	o	o	x
SMB Advanced Box	x	x	o	o	o	x

Wireless LAN

Canon imageRUNNER ADVANCE systems support wireless networking. Third generation imageRUNNER ADVANCE devices now come standard with Wireless LAN support. Wireless LAN is IPv6 compliant and supports the latest wireless encryption standards, including WEP, WPA and WPA2, in addition to support for the IEEE802.1X authentication standard.

The first generation and second generation imageRUNNER ADVANCE models can connect to wireless networks via the Silex Wireless Bridge SX-2500CG. This device includes security features such as Open System or Shared Key support with Wired Equivalent Privacy (WEP) encoding, WPA (Wi-Fi Protected Access) Personal (WPA-PSK) with a choice of TKIP or AES encryption methods, and WPA2, which adds Advanced Encryption Standard (AES) to encryption.

04

Network Security

IEEE 802.1X (Wireless and Wired supported)

Canon imageRUNNER ADVANCE systems support IEEE 802.1x, which 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.

IEEE 802.1X functionality is already supported by many Ethernet switches, and can prevent guest, rogue, or unmanaged systems that cannot perform a successful authentication from connecting to your network.

Dual-Line

Only available on Third Generation and imageRUNNER ADVANCE DX series

By setting wireless LAN as a sub-line in addition to wired LAN, it is possible to use the wired LAN and the wireless LAN in infrastructure mode at the same time.

Wireless LAN direct mode and wired LAN can operate at the same time.

Wireless LAN infrastructure mode and wireless LAN direct mode can operate at the same time.

With the sub-line, the following functions available in main line cannot be used:

Gateway setting, DNS name resolution, IPv6 communication, AutoIP setting, 802.1X authentication, IPsec and send/receive filter setting using arbitrary rule.

Sub-line allows access for specific communication only.

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

- CPCA (UDP 47545 for both transmission and reception, TCP 9013 for both transmission and reception)

The imageRUNNER ADVANCE provides separation between the Primary LAN and Secondary LAN preventing the routing of data between the two. As such, nodes connected to both LANs, which are different networks, are unable to communicate with each other through this device, directly or indirectly.

04

Network Security

Certificate Issue Request Function (Simple Certificate Enrollment Protocol: SCEP)

Certificate issue request function is a function for the device (MFD), which is a client, to obtain a public key certificate to certificate management server.

SCEP is used as the protocol to exchange data via network. In the following, the certificate management server to send certificate issue request to is called a SCEP server.

This function is used, in cases, for example, where device key pair used by a large amount of devices is updated automatically without a direct intervention of an administrator to reduce the management cost of the administrator. In an environment where IEEE802.1X communication is made by using device key pair issued from in-house certificate management server (SCEP server), there are certificates that expire in a short time such as in several months. In such cases, it is possible to update MFD at specified time using a timer rather than to update MFD one by one manually from remote UI.

Certificate issue request function has the following functionalities:

- Perform communication setting required for certificate issue request function, setting for key certificate and setting for timer from remote UI.
- Based on the instruction from the remote UI, the device generates key pair and CSR (Certificate Signing Request), sends such data to SCEP server as the certificate issue request (in data format PKCS#7) by SCEP, and registers it to the device as the certificate associated with the key pair generated when the certificate issue request is sent after receiving a public key certificate from SCEP server.
- At the time set by the timer, the device sends a certificate issue request to SCEP server with the same means as described above, receives a certificate from SCEP server and registers it to the device.

OCSP (Online Certificate Status Protocol)

Only available on Third Generation and imageRUNNER ADVANCE DX series and imagePRESS C165.
Requires Unified Firmware Platform (UFP) v3.10

To comply with RFC6960, the OCSP client feature is supported to allow real time validation of certificate revocation status online. A new OCSP function is added to Settings/Registration (both Local UI/remote UI). Previously, it needed to register the Certificate Revocation List (CRL) in the device, when checking validity of the certificate revocation status for an encryption protocol (TLS). With OCSP function, the device does not need to have a CRL (Certificate Revocation List) to validate the certificate status in real time.

04

Network Security

Embedded Web Browser

This WEB browser displays the HTML contents obtained from a WEB server on the user interface of the copier's control panel. This Web browser uses "WebKit" as the rendering engine.

The following security-related settings are available:

- TLS Version
- Using of JavaScript
- Displaying HTTPS/HTTP-mixed Pages

SNMP Community String

Community Strings are like passwords for the management elements of network devices. There is a community string which is used for read-only access to a network element. The default value for this community string for most network devices is often "public". Using this community string an application can retrieve data from the imageRUNNER ADVANCE system's Management Information Base (MIB) elements. There is also a read-write community string, and its default value is usually "private." Using the read-write community string, an application can actually change values for MIB variables.

Canon imageRUNNER ADVANCE systems use public and private as the default SNMP community strings, but these may be renamed to a user-defined value to provide some obfuscation. In addition, the systems support SNMPv3, which provides greater security by protecting data against tampering, ensuring access is limited to authorized users through authentication and encrypting data sent over a network.

To modify SNMP community strings go to Settings / Registration > Preferences > Network > SNMP Settings.

04

Network Security

Scan and Send - Virus Concerns for E-mail Reception

For imageRUNNER ADVANCE systems with Scan and Send capabilities enabled, the device will always discard any attached viruses in e-mail messages upon receipt.

Scan and Send-enabled devices support POP3 and SMTP as e-mail reception protocols. When data is received, the e-mail text is separated from any file attachments, and only JPEG/TIFF image files among the attached files are printed and transferred.

There are three possible scenarios that are explored:

- **Data with a virus attached in the e-mail:**

All file attachments except for 'JPEG/TIFF' files received in the e-mail are discarded immediately after reception.

- **Viruses pretending to be JPEG/TIFF files:**

The imageRUNNER ADVANCE system compresses the 'JPEG/TIFF' format at reception and after regenerating the image encodes the image again. When processed correctly, the original image is discarded and a new image is created, printed, and transferred. If an error occurs during the process, the data from the 'JPEG/TIFF' file is not transferred but is discarded, and a message notifying the user of the error is added to the e-mail text and is printed.

- **Text within e-mail is a virus:**

E-mail text data gives the Date, From, Message-Id, To, or Subject data written at the top of the received e-mail for printing and transfer. The e-mail text data is comprised of character strings. If binary data such as data with a virus is used in the e-mail text, the data will be damaged and data with a virus will be discarded. Even if the data with a virus is visible data with a script format, it is not possible to recognize it as a script because Date, From, Message-Id, To, or Subject data is attached at the top.

Mail Server Security

When the Scan and Send on imageRUNNER ADVANCE devices is enabled, the internal mail service is enabled and supports the POP, SMTP APOP, SMTP over SSL, POP3 over SSL protocols. To protect the service against attack or improper use, administrators can enable additional security features such as SMTP Authentication and POP Authentication before SMTP.

04

Network 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.

POP Authentication before SMTP

As an additional layer of security, imageRUNNER ADVANCE systems support the ability for administrators to 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.

05

Security Monitoring & Management Tools

Canon provides a number of tools to help organizations enforce their internal company policies and meet regulatory requirements. Whether a single imageRUNNER ADVANCE system is deployed, or a fleet of them, these solutions provide the ability to audit usage and limit access to features and functions enterprise-wide—at the group and user-level.

Security Policy Settings

As document, user, and information security become 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. Third generation imageRUNNER ADVANCE models have a centralized location, accessible using the Remote User Interface, where administrators are able to do the following:

- Set passwords for access to security policy settings
- Access and review current security settings
- Edit and save changes to security policies
- Export security settings and push updates to other third generation imageRUNNER ADVANCE models.

This functionality enables organizations the ability to separate security administration and device administration. Device administrators wouldn't automatically have access to security settings once a password is created.

Third generation imageRUNNER ADVANCE models have a centralized location where security administrators can access and manage various security settings. This is accessible from the Remote User Interface, where administrators are able to do the following

Security Policy Settings can be established for one device then exported as a file for use with other devices, or shared using iW EMC + Device Configuration Management Plug-in.

05

Security Monitoring & Management Tools

Security Policy Settings

imageWARE Enterprise Management Console

imageWARE Enterprise Management Console (EMC) is a highly scalable web-based management utility for administrators that delivers a streamlined, centralized point of control for all devices installed across enterprises. The software makes it easier for organizations to securely manage one or more imageRUNNER ADVANCE systems remotely across a network. To aid in implementing and managing an MFD infrastructure, imageWARE Enterprise Management Console facilitates the secure distribution of device configuration information and address books using SSL encryption.

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.

Device Application Management Plug-in

Enables MEAP applications to be updated, managed, and deployed remotely to a fleet with a single procedure.

Device Firmware Update Plug-In

Allows administrators to push out firmware updates to the fleet.

Security Policy Management Plug-In

Provides security policy monitoring by delivery task schedule and its settings.

Credential Management Plug-In

Enables to maintain certificates and password and is useful to keep settings that could impact device security up to date.

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.

Access Management System

The Access Management System enables the ability for administrators to restrict access to the features of the system at the device or function level. If device authentication is used, users will need to login prior to accessing the Main Menu. If Function Level Authentication in the Access Management System is used, users will be prompted for their credentials to use certain, often sensitive device features.

06

Logging & Auditing

Few security procedures can completely prevent the intentional leak of confidential information while maintaining high productivity, but if an occurrence does happen it is important to be able to trace it to the source. Canon has implemented a number of technologies to provide administrators with powerful ways to discourage leaks and investigate unauthorized access.

Audit Log

An audit log is a chronological sequence of audit records to automatically track every action undertaken by users, developers, and administrators for the system (Who does what and when?). These records are used to monitor system usage to determine compliance with regulations, security standards, enterprise policies, etc., as well as to prove usage effectiveness as audit trails.

The following logs are available:

- User authentication log/user management log
- Network connection log IPSec/TLS (only for Third Generation imageRUNNER ADVANCE)
- Mail Box authentication/document operation log
- Advanced Box save document operation log
- MEAP application management log (4200/C3300/Third Generation supported)
- Software registration/update log
- Mail Box backup log
- Device management log (device startup/shutdown log, user mode setting change log, key certification/operation log, data import/export log, access privileges change for SNMP V3 MIB that contains user information)
- Job history log
- Send/receive data log
- Audit/management log
- Import/export data log

06

Logging & Auditing

From the imageRUNNER ADVANCE 4200 series onward, the following audit logs are supported.

SSL network connection log	Log when SSL negotiations fail
Service mode operation log	Log when some operations are performed in the service mode
System maintenance log (only for C3300 and Third Generation imageRUNNER ADVANCE)	Log of operations performed when starting in the safe mode Log of installing updates and MEAP applications from USB
S/MIME certificate log	Log of registering/generating/deleting certificates for S/MIME
DCM data log	Log of importing/exporting additional categories
Authenticated print log	Log of storing/deleting documents with authenticated print
Group management log	Log of managing group information
Security policy log	Log of authenticating and registering the security policy password
Settings/Registration operation log	Log of using additional Settings/Registration items

Note: - The Mail Box backup log is not supported on the imageRUNNER ADVANCE C3300/C350/C250/C2200/500/400 series.

Audit Log Management

Audit Log Collection feature has 3 main functions:

1. Audit Log Management Function

Uses the Esplet function to collect the audit logs that are stored within the device, which it then stores in its own storage area. The Audit Log Management Function also provides a log deletion function.

2. Audit Log Export Function

Provides a means for the stored logs to be exported into a CSV-format file, using the Servlet function. The resulting CSV file can then be used by the administrator as a basis for auditing based on the usage records from the device.

3. Audit Log Syslog Send Function

06

Logging & Auditing

Audit Log Syslog Send Function

Audit Log Collection feature has 3 main functions:

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.

If audit log collection is made while “Use Syslog Send” is checked, Syslog Send process of log is performed. (Settings/Registration > Management Settings > Device Management > Export/Clear Audit Log > Syslog Settings)

At that timing, audit log collection process is performed first. Then, collected audit logs are sent to Syslog server using selected protocol (TCP/UDP/TCP (TLS)). Even if Syslog Send is enabled, it is still possible to make manual/automatic export.

The format of Syslog message to be sent conforms to RFC5424 and has the following structure:

HEADER SP STRUCTURED-DATA SP MSG

SP: space

[HEADER part]

HEADER part consists of the followings:

<PRI> VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID

- PRI: (Facility value selected by user) * 8 + Severity value (level of importance. If the result column of the audit log is OK, Info: 6. If no good, Error: 3)

-> If LPR is selected and the log is OK, it will be $6 * 8 + 6 = 54$.

- VERSION: A numeric value “1” is entered

- TIMESTAMP: The value of the time column of the audit log is obtained and converted to UTC format

-> Example: 2017-08-07T12:00:00Z

- HOSTNAME: IP address of the device (sender)

- APP-NAME PROCID: Unused and “-” (hyphen) is placed

- MSGID: Audit log number

[STRUCTURED-DATA part]

STRUCTURED-DATA part is not used, thus “-” (hyphen) is placed.

imageWARE Secure Audit Manager Express (iW SAM Express)

Canon imageWARE Secure Audit Manager Express (iWSAM) is an optional security solution as part of uniFLOW. In combination with uniFLOW (on premise) solutions, iW SAM Express allows to monitor on job logs and image data and allows to set alerts based on specific rules of document distribution indicated by the administrator. This permits to monitor if documents are shared outside of access permissions and take measures to correct for any unpermitted access to documentation.

07

Canon Solutions & Regulatory Requirements

Canon is dedicated to providing the most secure multifunctional printers available on the market today. Many of our products meet or exceed the requirements of government agencies and private entities as they relate to security certifications and industry regulations.

Common Criteria

The US 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.

ISO 15408 (otherwise known as Common Criteria (CC)) is an international standard for computer security certification developed by governments of the U.S., U.K., Canada, Germany, France and the Netherlands. It provides assurance that IT security has been evaluated with a unified defined set of criteria commensurate to the target environment for use. The agreement between countries 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.

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 (EALs), against which products' functions are tested and evaluated.

EALs 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.

07

Canon Solutions & Regulatory Requirements

IEEE 2600 Common Criteria Certification

IEEE Std. 2600 TM-2009 or “IEEE Standard for a Protection Profile in Operational Environment A/B” (referred to as IEEE 2600, hereafter) Protection Profile is a global information security standard for hard copy devices that require a relatively high level of document security, operational accountability and information assurance. IEEE 2600 defines requirement specifications for office use as well as government agencies where high level of assurance is required. The IEEE 2600 Common Criteria certification evaluates whether security functions provided by products and technology are properly implemented. The IEEE 2600 Protection Profile is part of a suite of standards developed by the Hardcopy Device and System Security Working Group, sponsored by the IEEE Information Assurance Standards Committee of the IEEE Computer Society. Canon participated in the development of the P2600 suite of Protection Profiles as a member of the Hardcopy Device and System Security Working Group.

With specified processes, configurations and settings implemented upon installation, the imageRUNNER ADVANCE line will be certified within 6 months of each product launch, to achieve and maintain the necessary security requirements as defined in the IEEE 2600 standard.

Certified Device- Canon’s imageRUNNER ADVANCE models can be considered an IEEE 2600 CC Certified model when the following options are installed and active on the device:

- iR-ADV Security Kit for IEEE 2600
 - o IEEE 2600 License Certificate
 - o Bootable CD with certified system software
 - o IEEE 2600 User Manual CD
 - o Installation Manual
- HDD Data Encryption & Mirroring Kit standard on Third Generation imageRUNNER ADVANCE products.

After installation and configuration is completed, an end user can verify and check a device configuration screen to verify that it is an IEEE 2600 Common Criteria certified configuration.

Please note, various settings made at installation might require disabling functions or features of the device to achieve and maintain certification.

Given the common controller architecture used by Canon’s imageRUNNER ADVANCE architecture, the imageRUNNER ADVANCE Series models, when equipped with necessary accessories, along with specific installations and configurations, can be considered compliant with the IEEE 2600 standard, although they have not been submitted for certification.

08

Conclusion

Since initially introduced, the Canon printers and MFPs have grown in both the breadth and depth of features and functions. As with any networked device, imaging and printing devices must be included within the broader context of the company's overall security strategy to help ensure the confidentiality, integrity and availability of information.

When properly deployed, the devices can be effectively protected against vulnerabilities from either malicious or unintentional use. Combined with advanced monitoring and management tools for auditing and centralized administration, the systems can meet the demand for increased productivity and strong security.

Each customer's needs are different, and while the security of corporate data is ultimately the responsibility of the customer, Canon can offer additional services and expertise to enhance the security levels, from device initial set-up to its end of life. While these suggestions assist in enhancing device security, internal company security policies should ultimately dictate which security measures are appropriate for implementation within a specific environment.

1. Security-related services

Canon offers services focused on enhancing the protection of your information, especially useful when there's a lack of in-house expertise or resources.

2. Device hardening service

Offering pre-configuration of security focused settings and functions on your i-SENSYS or imageRUNNER device before it is delivered and connected to your network.

3. Data removal service

Offering permanent deletion of both physical and digital data when devices reach end-of-life, including documented evidence upon completion of service.

Canon is committed to helping our customers meet their objectives related to security of their critical information and is continuing to develop new technologies in this area. For more information, please visit:

<https://www.canon-europe.com/support/product-security>

Please find model-level detail regarding security support on the available Security Matrix document.

Canon Security Recommendations Quick Reference

Each customer's needs are different, and while the security of corporate data is ultimately the responsibility of the customer, the security technologies outlined below may help support your organization's information security needs. The following actions are recommended by Canon as appropriate first steps in securing an imageRUNNER ADVANCE system for most environments. Canon offers an MFD Hardening Guide that details the configuration options to provide sufficient information to enable you to discuss the most appropriate settings for your environment. For more information please contact your Canon representative.

1. Choose a form of User Authentication and/or Access Control
2. Set the system administrator ID and password
3. Disable unused ports and applications (e.g. FTP, RUI)
4. Set passwords for Mail Boxes and Advanced Boxes
5. Restrict printing and RUI access to specific IP or MAC addresses
6. Set passwords for Address Book management
7. Change the SNMP community strings
8. Disable the USB port if unused
9. Utilize Optional Hard Disk Drive Erase Kit or Hard Disk Drive Encryption Kit to ensure integrity of data stored on internal Hard Disk Drives
10. Monitor the devices using imageWARE EMC

While these suggestions assist in enhancing device security, internal company security policies should ultimately dictate which security measures are appropriate for implementation within a specific environment.

Canon imageRUNNER ADVANCE Security Features Supported Device List

Product Family	Second Generation imageRUNNER ADVANCE	Third Generation imageRUNNER ADVANCE
Security Features	C9200 Series, C7200 Series, C5200 Series, C3300 Series, C2200 Series, C350iF/C250iF, 8200 Series, 6200 Series, 4200 Series, 500iF/400iF	C7500 Series, C5500 Series, C3500 Series, C355/C255iF, 8500 Series, 6500 Series, 4500 Series
Security Management		
Security Policy Settings	NA	Standard
Device Based Authentication		
Device-Based	Standard	Standard
Active Directory/SSO	Standard	Standard
Universal Login Manager	Optional	Standard
Card Based Authentication		
Proximity Card or CAC/PIV	Optional	Optional
Access Control		
Password Protected System Setting	Standard	Standard
Access Management System	Standard	Standard
USB Block	Standard	Standard
Data Security		
TPM (Trusted Platform Module)	Standard	Standard
Hard Drive Password Lock	Standard	Standard
Hard Drive Data Format (EOL)	Standard (9x)	Standard (9x)
Hard Drive Data Erase	Standard	Standard
Hard Drive Data Erase Scheduler MEAP	Optional *	Optional
Hard Drive Data Encryption	Optional (Common Criteria Certified)	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE2600 Common Criteria)**	Optional (IEEE2600 Common Criteria)**
Removable Hard Drive Kit	Optional ***	Optional ***
Document Security		
Secure Print (Driver Based)	Standard	Standard
Secure Print (Server/Serverless)	Optional	Optional
Mail Box Security	Standard / NA ▲	Standard
Encrypted PDF	Optional	Optional
Document Scan Lock	Optional <1	Optional
Network Security		
Port Management, IP Address & MAC Filtering	Standard	Standard
IPSEC	Standard	Standard
Cipher Algorithm Selection	NA	Standard
TLS1.1/1.2/1.3 Support and SSL3.0 Disabled	NA ▲ ▲	Standard
FTPS	NA	Standard
Certifications		
Common Criteria IEEE 2600	Optional/NA	Optional **
FIPS 140-2	IPSEC/CAC/PIV	IPSEC/CAC/PIV/HDD Encryption/TLS

* imageRUNNER ADVANCE C5200 Series with firmware V 17.10 or higher.

** IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.

*** Not available with the imageRUNNER ADVANCE 500iF/400iF and C350iF/C250iF Series.

▲ Not available with the imageRUNNER ADVANCE C2200 Series, 500iF/400iF, and C350iF/C250iF Series.

▲ ▲ Not available with the imageRUNNER ADVANCE C2200 Series, 8200 Series, 6200 Series, and 4200 Series

09

Appendix

Product Family	Third Generation imageRUNNER ADVANCE	Third Generation imageRUNNER ADVANCE 2nd Edition
Security Features	C7500 Series, C5500 Series, C3500 Series, C355/C255iF, 8500 Series, 6500 Series, 4500 Series	C7500 II Series, C5500 II Series, C3500 II Series, C356iF II Series, 8500 II Series, 6500 II Series, 4500 II Series, 715iF II Series
Security Management		
Security Policy Settings	Standard	Standard
Device Based Authentication		
Device-Based	Standard	Standard
Active Directory/SSO	Standard	Standard
Universal Login Manager	Standard	Standard
Card Based Authentication		
Proximity Card or CAC/PIV	Optional	Optional
uniFLOW Online Express	Able to upgrade	Standard
Access Control		
Password Protected System Setting	Standard	Standard
Access Management System	Standard	Standard
USB Block	Standard	Standard
Data Security		
TPM (Trusted Platform Module)	Standard	Standard
Hard Drive Password Lock	Standard	Standard
Hard Drive Data Format (EOL)	Standard (9x)	Standard (9x)
Hard Drive Data Erase	Standard	Standard
Hard Drive Data Erase Scheduler MEAP	Optional	Optional
Hard Drive Data Encryption	Standard (FIPS 140-2 Validated)	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE2600 Common Criteria)**	Optional (IEEE2600 Common Criteria)**
Removable Hard Drive Kit	Optional / NA **	Optional / NA **
Document Security		
Secure Print (Driver Based)	Standard	Standard
Encrypted Secure Print (Driver Based)	Optional	Standard
Secure Print (Server/Serverless)	Optional	Optional
Secure Watermark	Optional	Standard
Mail Box Security	Standard	Standard
Encrypted PDF (AES 256 support)	Optional	Standard
Device Digital Signature PDF	Optional	Standard
Document Scan Lock	Optional	Optional / NA ***
Network Security		
Port Management, IP Address & MAC Filtering	Standard	Standard
IPSEC	Standard	Standard
Cipher Algorithm Selection	Standard	Standard
TLS1.1/1.2/1.3 Support and SSL3.0 Disabled	Standard	Standard
FTPS	Standard	Standard
Certifications		
Common Criteria IEEE 2600	Optional *	Optional *
FIPS 140-2	IPSEC/CAC/PIV/HDD Encryption/TLS	IPSEC/CAC/PIV/HDD Encryption/TLS

*IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.

** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF, C355iF/C255iF and C356iF II/C256iF II Series.

*** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF.

09

Appendix

Product Family	Third Generation imageRUNNER ADVANCE 2nd Edition	Third Generation imageRUNNER ADVANCE 3rd Edition, imagePRESS Lite
Security Features	C7500 II Series, C5500 II Series, C3500 II Series, C356iF II Series, 8500 II Series, 6500 II Series, 4500 II Series, 715iF II Series	C7500 III Series, C5500 III Series, C3500 III Series, C356iF III Series, 8500 III Series, 6500 III Series, 4500 III Series, 715iF III Series, C475iF III Series, C165
Device Management		
Verify System at Startup	NA	Standard
McAfee Embedded Control	NA	Standard
Security Management		
Security Policy Settings	Standard	Standard
Device Based Authentication		
Device-Based	Standard	Standard
Active Directory/SSO	Standard	Standard
Universal Login Manager	Standard	Standard
Card Based Authentication		
Proximity Card or CAC/PIV	Optional	Optional
uniFLOW Online Express	Standard	Standard
Access Control		
Password Protected System Setting	Standard	Standard
Access Management System	Standard	Standard
USB Block	Standard	Standard
Data Security		
TPM (Trusted Platform Module)	Standard	Standard
Hard Drive Password Lock	Standard	Standard
Hard Drive Data Format (EOL)	Standard (9x)	Standard (9x)
Hard Drive Data Erase	Standard	Standard
Hard Drive Data Erase Scheduler MEAP	Optional	Optional
Hard Drive Data Encryption	Standard (FIPS 140-2 Validated)	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE2600 Common Criteria)*	Optional (IEEE2600 Common Criteria)*
Removable Hard Drive Kit	Optional / NA **	Optional / NA **
Document Security		
Secure Print (Driver Based)	Standard	Standard
Encrypted Secure Print (Driver Based)	Standard	Standard
Secure Print (Server/Serverless)	Optional	Optional
Secure Watermark	Standard	Standard
Mail Box Security	Standard	Standard
Encrypted PDF (AES 256 support)	Standard	Standard
Device Digital Signature PDF	Standard	Standard
Document Scan Lock	Optional / NA ***	Optional / NA ***
Network Security		
Port Management, IP Address & MAC Filtering	Standard	Standard
IPSEC	Standard	Standard
Cipher Algorithm Selection	Standard	Standard
TLS1.1/1.2/1.3 Support and SSL3.0 Disabled	Standard	Standard
FTPS	Standard	Standard
Certifications		
Common Criteria IEEE 2600	Optional *	Optional *
FIPS 140-2	IPSEC/CAC/PIV/HDD Encryption/TLS	IPSEC/CAC/PIV/HDD Encryption/TLS

*IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.

** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF, C356iF, C475iF Series.

*** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF, C475iF Series.

09

Appendix

Product Family	Third Generation imageRUNNER ADVANCE 3rd Edition, imagePRESS Lite	imageRUNNER ADVANCE DX
Security Features	C7500 III Series, C5500 III Series, C3500 III Series, C356iF III Series, 8500 III Series, 6500 III Series, 4500 III Series, 715iF III Series, C475iF III Series, C165	C7700 Series, C3700 Series, 8700 Series, 6700 Series, 4700 Series
Device Management		
Verify System at Startup	Standard	Standard
McAfee Embedded Control	Standard	Standard
Security Management		
Security Policy Settings	Standard	Standard
Device Based Authentication		
Device-Based	Standard	Standard
Active Directory/SSO	Standard	Standard
Universal Login Manager	Standard	Standard
Card Based Authentication		
Proximity Card or CAC/PIV	Optional	Optional
uniFLOW Online Express	Standard	Standard
Access Control		
Password Protected System Setting	Standard	Standard
Access Management System	Standard	Standard
USB Block	Standard	Standard
Data Security		
TPM (Trusted Platform Module)	Standard	Standard
Hard Drive Password Lock	Standard	Standard
Hard Drive Data Format (EOL)	Standard (9x)	Standard (9x)
Hard Drive Data Erase	Standard	Standard
Hard Drive Data Erase Scheduler MEAP	Optional	Optional
Hard Drive Data Encryption	Standard (FIPS 140-2 Validated)	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE2600 Common Criteria)*	Optional (IEEE2600 Common Criteria)*
Removable Hard Drive Kit	Optional / NA **	NA ***
Document Security		
Secure Print (Driver Based)	Standard	Standard
Encrypted Secure Print (Driver Based)	Standard	Standard
Secure Print (Server/Serverless)	Optional	Optional
Secure Watermark	Standard	Standard
Mail Box Security	Standard	Standard
Encrypted PDF (AES 256 support)	Standard	Standard
Device Digital Signature PDF	Standard	Standard
Document Scan Lock	Optional / NA ***	NA
Network Security		
Port Management, IP Address & MAC Filtering	Standard	Standard
IPSEC	Standard	Standard
Cipher Algorithm Selection	Standard	Standard
TLS1.1/1.2/1.3 Support and SSL3.0 Disabled	Standard	Standard
FTPS	Standard	Standard
Certifications		
Common Criteria IEEE 2600	Optional *	Optional *
FIPS 140-2	IPSEC/CAC/PIV/HDD Encryption/TLS	IPSEC/CAC/PIV/HDD Encryption/TLS

*IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.

** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF, C356iF, C475iF Series.

*** Not available with the imageRUNNER ADVANCE 715iF/615iF/525iF, C475iF Series.

**** There is no Removable HDD Data Kit option for imageRUNNER ADVANCE DX series. However, DX models (excluding C3700 series) can remove HDD when connector reaches life service parts to replace the connector must be purchased.

09

Appendix

IEEE 2600 CC Functional Requirements

	Functional Requirements	Purpose	Functions supported by iR-ADV
1	User recognition/authentication function	To prevent unauthorized use by unregistered persons	User Authentication (UA)
2	Access control of device function	To prevent an unauthenticated user from executing the digital MFD functions for which the user does not have the privilege.	AMS: Access Management System
3	Remaining data deletion function	To prevent temporary data in a device (such as image data generated by a job) from being reused	HDD complete deletion function
4	Protection function for user data in the nonvolatile memory (such as HDD)	To prevent leakage of information due to the HDD unit taken away	HDD encryption function
5	Protection function for network data	To prevent LAN data from being stolen	IPsec
6	Protection function for user data transfer	To counter the attacks by the abuse of Fax	Stop a transfer function
	Access control function for jobs	Blocking invalid access to a user document	Controlling access to inboxes by password and printing by storing a job due to secured print
7	Audit log generation function	To audit user operation	Job log/User authentication log/Mail Box operation log/Device management log
8	Self-test function	To ensure that the main security functions are normal	Self-test of encryption module

10

Disclaimer

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 partners, 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.

Regulatory Disclaimer:

Statements made in this document are the opinions of Canon Europe. None of these statements should be construed to customers or Canon Europe's partners as a legal advice, as Canon Europe does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes Oxley or the GDPR. Each customer must have its own qualified counsel determine the suitability of a particular solution for the regulatory and statutory compliance.

All specifications and availability are subject to change without notice.

Canon Inc.
canon.com

Canon Europe Ltd.
canon-europe.com

English Edition

© Canon Europa N.V. 2020

Canon
