Canon

White Paper: Canon imageRUNNER ADVANCE Security

INTENT OF THIS DOCUMENT:

Canon recognizes the importance of information security and the challenges that your organization faces. This white paper provides information security facts for Canon imageRUNNER ADVANCE systems. 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 administrative personnel responsible for the configuration and maintenance of imageRUNNER ADVANCE systems. The information in this document, in conjunction with other best practices, may be used as guidance to help improve your organization's overall security. Some security settings may affect device functionality or performance. You may want to test these settings before deploying them in your environment to ensure you understand their effects.

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 review in this white paper include both standard and optional solutions for imageRUNNER ADVANCE systems. Specifications and availability subject to change without notice.

Table of Contents

Section 1 — Introduction

"If you look at these machines as just copiers or printers, you first wonder if you really need security. Then you realize conventional office equipment now incorporates significant technology advances and capabilities that make all documents an integrated part of a corporate network that also involves the Intranet and Internet. Government agencies, corporations and non-profits are increasingly transitioning from traditional stand-alone machines to devices that integrate these functions and link them to corporate networks, raising a whole new era of information management and security issues.

Our development of features within Canon imageRUNNER ADVANCE systems are designed to help prevent data loss, help protect against unwanted device infiltration and help keep information from being compromised."

> —Dennis Amorosano, Sr. Director
>   Solutions Marketing & Business Support, Canon U.S.A., Inc.

As the marketplace has evolved, the technology associated with office equipment continues to develop at an ever-increasing pace. Over the last several years alone, traditional office equipment has leapfrogged in technology, expanding its functional capabilities, while at the same time becoming an integral part of the corporate network and the Internet. As a result, a new level of security awareness has become imperative.

Canon's attention to emerging market trends and details surrounding customer security requirements has driven the development of features within imageRUNNER ADVANCE systems, which has been designed to help thwart data loss and the potential threats posed by hackers.

Section 1 — Introduction

1.1 — Security Market Overview

In today's digital world, risks to networks and devices come in more forms and from more directions than ever before. From identity theft and intellectual property loss to infection by viruses and Trojan horses, IT administrators today find themselves playing an additional role of security officer 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 MFPs, 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 Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA) and Family Education Rights Privacy Act (FERPA) all require that IT administrators ensure the security, privacy, accuracy and reliability of information receives the utmost attention.

1.2 — Imaging & Printing Security Overview

Today's multifunction devices share many similarities with general purpose PCs. They contain many of the same components like CPUs, memory and hard disks; and some even use mainstream operating systems like Windows or Linux. Like any other device on the network, sensitive information may be passed through these units and stored in the device's hard disk and memory. Yet at many companies multifunction devices are not given the same attention concerning information security.

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.

1.3 — 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
- Information Security
- Network Security
- Security Monitoring / Management Tools
- Logging & Auditing

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

Section 2 — Device Security

2.1 – imageRUNNER ADVANCE Controller Security

The imageRUNNER ADVANCE series is built upon a new platform that provides powerful enhancements to security and productivity. The new architecture centers on a new 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.

2.2 – 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 color output, and total print counts by department or user.

Device-Based Authentication

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 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 (SSO) and SSO Hybrid (SSO-H) Login
Single Sign On (SSO) is a 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 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.

SSO ships 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.

Section 2 — Device Security

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.

Card-Based Authentication

uniFLOW Card Authentication
When combined with the optional uniFLOW Output Manager Suite, 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.

Advanced Authentication—Proximity Card
Using a MEAP application, imageRUNNER ADVANCE systems can be customized to automatically perform user authentication with contactless cards typically used in corporate environments. User data can be stored locally in a secure table to eliminate the need for an external server, or integrated with an existing authentication server through customization. Support is provided for cards from HID Prox, HID iClass, Casi-Rusco, MIFARE and AWID. Customization can also be performed to provide support for other card types.

Authorized Send for CAC/PIV
To fulfill the strict security requirements of government agencies as dictated by Homeland Security Presidential Directive-12 (HSPD-12), imageRUNNER ADVANCE systems support the use of Common Access Card (CAC) and/or Personal Identity Verification (PIV) card authentication for the embedded Authorized Send MEAP application. Authorized Send for CAC/PIV is a server-less application that protects the Scan-to-Email, Scan-to-Network Folder and Scan-to-Network Fax functions, while allowing general use of walk-up operations like print and copy.

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

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

Control Cards/Card Reader System
Canon imageRUNNER ADVANCE systems offer support for an optional Control Card/Card Reader system for device access and to manage usage. The Control Card/Card Reader system option requires the use of intelligent cards that must be inserted in the system before granting access to functions, which automates the process of Department ID authentication. The optional Control Card/Card Reader system manages populations of up to 300 departments or users.

Section 2 — Device Security

2.3 – 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. Access control solutions for the imageRUNNER ADVANCE can help Authentication, Authorization, and Auditing. 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.

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.

System Manager Screen

Store ID and Password Screen

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.

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. The administrator can also define whether to allow unregistered users to log in as guests and then specify settings for guest user's roles.

Section 2 — Device Security

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 devise 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:

Device Function	Values	Description
Print	Allowed, Not Allowed	Allows or prohibits using applications related to the Print function.
Copy	Allowed, Not Allowed	Allows or prohibits using applications related to the Copy function.
Send/Store on Network		Sets restrictions for externally sending scanned documents, user inbox documents, and saving documents to file servers or network storage.
E-mail TX	Allowed, Not Allowed	Allows or prohibits sending via E-mail TX.
I-Fax TX	Allowed, Not Allowed	Allows or prohibits sending via I-Fax TX.
Fax TX	Allowed, Not Allowed	Allows or prohibits sending via Fax TX.
FTP TX	Allowed, Not Allowed	Allows or prohibits sending via FTP TX.
NetWare (IPX) TX	Allowed, Not Allowed	Allows or prohibits sending via NetWare (IPX) TX.
Windows (SMB) TX	Allowed, Not Allowed	Allows or prohibits sending via Windows (SMB) TX.
WebDAV TX	Allowed, Not Allowed	Allows or prohibits sending via WebDAV TX.
Inbox TX	Allowed, Not Allowed	Sets restrictions for saving scanned documents to user inboxes.
Specify Address Domain/Send to Addresses Received from Cell Phone	Allowed, Not Allowed	For imageRUNNER ADVANCE devices, these restrictions also apply to addresses received from cell phones.
Use Address Book/Register Storage Location for Network	No Restrictions, Not Allowed, Read-Only	For imageRUNNER ADVANCE devices, these restrictions also apply to registering, editing, and deleting network storage.
Send to New Addresses/Send to Addresses Received from Cell Phone	Allowed, Not Allowed	For imageRUNNER ADVANCE devices, these restrictions also apply to addresses received from cell phones.
Add Device Signature to Sending Files	Added, Not Added	Allows or prohibits adding of a device signature when sending PDF files.
Sending Files Format	Allowed, Not Allowed	Allows or prohibits sending file formats that a device signature cannot be added to.
Save Functions (Mailbox/Hold/Memory Media)	Allowed, Not Allowed	Allows or prohibits saving functions.
Web Access	Allowed, Not Allowed	Allows or prohibits using applications related to the Web Access function.
Utility	Allowed, Not Allowed	Allows or prohibits using applications related to Utilities.
Others	Allowed, Not Allowed	Allows or prohibits using other applications.
MEAP Applications	Allowed, Not Allowed	Allows or prohibits the use of MEAP applications.

* Requires SSO-H to be enabled.

Section 2 — Device Security

When the Access Management System has been enabled, users must log in to the device using SSO 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 grayed 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 SSO-H for authentication. It enables administrators to choose precisely which functions are permitted by walk-up and network users without entering credentials versus the ones that require a user to login. For example, administrators may choose to allow all users to make black-and-white copies while prompting users to login if they choose to output color or use the Scan and Send function.

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 same password is also used for the Address Book Import/Export function through the Remote UI utility.

* Requires imageWARE Enterprise Management Console and the Access Management System Plug-In when authenticating through Active Directory.

Address Book Password Screen

Address Book Access Code Enable/Disable Screen

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 › Register Destinations › Register New Destinations, from here the user can register an 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.

In addition to restricting all new destinations, administrators can also restrict the addition of new addresses for specific destination types that are available to users when sending documents with Scan and Send and Fax. Permissions can be set to enable or disable the entry of new addresses for the following:

- Entries in the Address Book
- LDAP Servers
- User Inboxes
- One-touch Buttons
- Favorites Buttons
- The User's E-mail Address (Send to Myself, if Using SSO Login)

Section 2 — 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 authorized to print. Printing restrictions can be set using Department ID credentials or through the Access Management System.

Custom Driver Configuration Tool
Administrators can create customer driver
profiles for users to limit access to print features and specify default settings, thereby protecting the device against unauthorized use, enforcing internal policies and better control output costs. Security conscious settings that can be defined and enforced include duplex output, secure print, B&W only on color devices, watermarks and custom print profiles, as well as hiding any desired functions. For easier deployment, the customized drivers can be distributed to desktops across the organization through the Printer Driver Management Plug-in for imageWARE Enterprise Management Console (iWEMC).

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.

2.4 – 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.

# Section 3 – Information 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.

3.1 – Document Security

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 minimizes unattended papers 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 optional Encrypted Secured Print software, security is further enhanced by using strong 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.
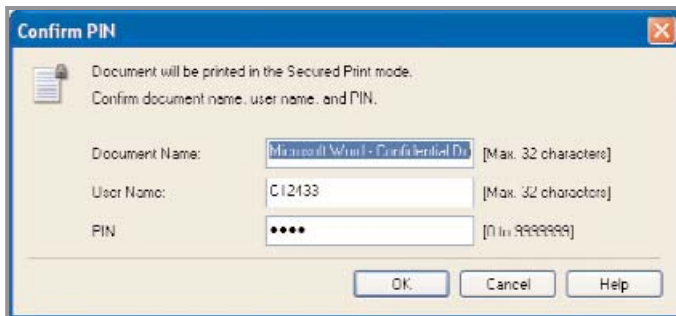
Secure Print screen from the Printer Driver
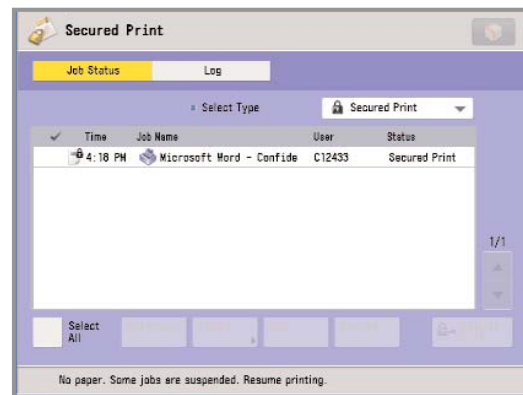
Print Job Status Screen

uniFLOW Secure Print
Exclusive to Canon is the uniFLOW Output Manager Suite, which is optional modular software to reduce costs, improve productivity and enhance security. From a security perspective, uniFLOW Output Manager Suite 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. Users can then access the uniFLOW MEAP client application from the device's control panel and release their job from their queue of pending documents.

* Requires the Encrypted Secure Print option.

Section 3 – Information Security

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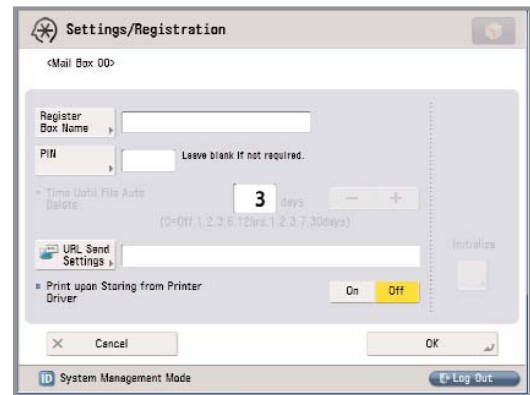
Mail Box Security
Each imageRUNNER ADVANCE system ships standard with Mail Boxes for storage of scanned and printed data. Mail Box security is provided by the ability to designate a unique password for access. Once a document is stored in the Mail Box (if the Mail Box is password protected), a user must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

Administrators can also use the Print Job Restriction feature to restrict direct printing from a desktop to the device. This forces all print jobs to be stored in a Mail Box before the user can output the print job at the device.
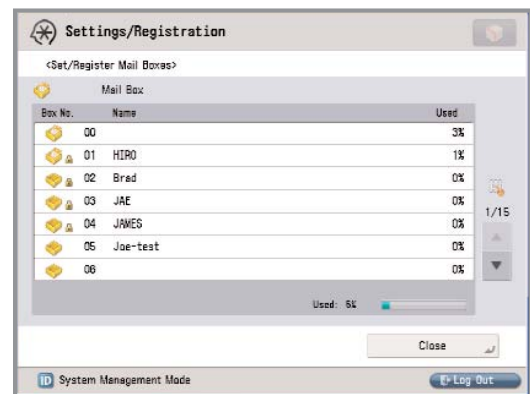
Advanced Box Security
The Advanced Box feature enables the imageRUNNER ADVANCE system to serve as a file sharing storage space. Users can save files in a shared folder, or within their own personal space in their native file format such as Word or PDF. Each user's personal space is protected with security 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.

Box Set/Store Password Screen

Mail Box Store Destination Screen

Mail Box Set/Store Password Screen

Section 3 – Information Security

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.

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.
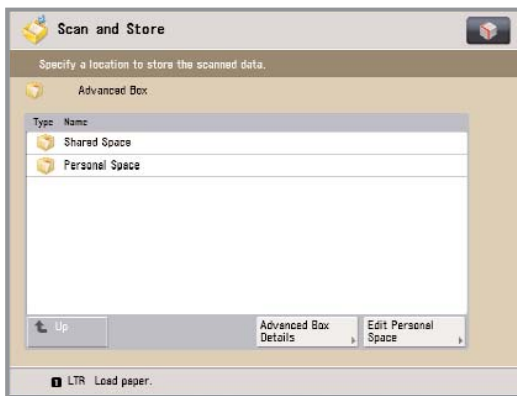
Advanced Box Scan and Store Screen
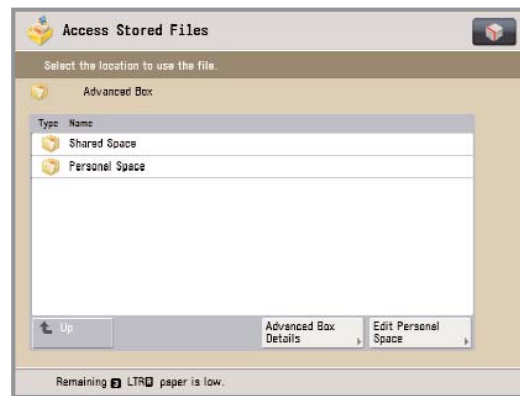
Advanced Box Access Stored Files Screen

Other 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 duplicated are made by photocopying, the secure watermark appears. The optional 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 preset watermarks to appear in any position on copied output.

Encrypted PDF
The Encrypted PDF mode within the optional Scan and Send Security Feature Set enables users to encrypt, set password and define permissions for PDF files that are sent to an e-mail address or file server for enhanced security. Only users who enter the correct password can open, print, or change the received PDF file.

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.

Section 3 – Information 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 and choose its position and orientation on the page. This not only makes the digital signature more prominent, but also ensures that the digital signature appears on any printed versions of the document.

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.

Adobe LiveCycle Rights Management ES*
In general, once a PDF is created it can be openly exchanged if it is unencrypted and/or not secured by a password. Organizations that require more precise control over their information can integrate an imageRUNNER ADVANCE system with an Adobe LiveCycle® Rights Management ES server. The Adobe LiveCycle Rights Management ES application makes it possible to enforce dynamic document policies for choosing the authenticated users that are authorized to view its contents, define expiration dates, track distribution and define watermarks. Once the document's privileges have been set, it will contact the Adobe LiveCycle® Rights Management server over the Internet to enforce the latest policy.

Document Scan Lock & Trace
The optional Document Scan Lock & Tracking feature of imageRUNNER ADVANCE systems enables documents to include embedded tracking information such as usernames, date stamps, and device name within the background. The embedded information is not readable by users, and can only be accessed by system administrators. The tracking information can also contain policy information that determines whether the document can be copied or scanned on another imageRUNNER ADVANCE systems with Document Scan Lock enabled.

Please refer to Section 6 — Logging & Auditing on page 30 for a more detailed description on the Document Scan Lock & Trace feature.

---

* The PDF/A-1b and Encrypted PDF file formats are not compatible with Adobe LiveCycle® Rights Management ES.

The Scan Lock feature enables the following restrictions to be applied to a document:

- Complete Restriction: No one can make any copy/send/fax.
- Password Authentication: Allows the ability to make copy/send/fax only if the proper password is entered.
- User Authentication: Allows the ability to make copy/send/fax only to original authorized user logged into the device with the proper User ID and Password.

System administrators can choose to force all scan and copy jobs to apply Document Scan Lock & Tracking code onto each print job, as well as choose whether to allow all or prohibit all copy, scan, send and fax jobs of documents that contain the hidden tracking code.

For more information on Document Scan Lock & Tracking as it pertains to tracing, please consult the *Logging & Auditing section* in this document.

3.2 – Data Security*

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 requirements of key customers and U.S. government agencies. Canon offers advanced security features that protect data stored on the device and during transmission.

Data at Rest

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 analyzing its data at the sector level is extremely difficult.

The "Fat-32 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 analyze the data on these file systems at the sector level, however, Canon recognizes that highly motivated and experienced attackers may try to obtain

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

information from environments, where sensitive information is processed, by analyzing 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, the HDD Data Encryption Kit or the Removable HDD Kit.

Standard HDD Format*

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 Format feature, which is standard on all imageRUNNER ADVANCE systems, is more than just a regular hard disk format function. It not only deletes the File Allocation table (FAT) associated with all user areas on the disk, but it also overwrites all user data areas on the hard disk with null characters. 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 and license files
- 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 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)

The standard HDD format feature that is included with every imageRUNNER ADVANCE system will perform a one pass overwrite using null characters. If the optional HDD Erase Kit is installed, the HDD Format feature provides additional overwrite options, including the choice to perform a DoD 5022.22M compliant 3-pass overwrite.

HDD Data Encryption Kit

The HDD Data Encryption Kit option, which has achieved Common Criteria Certification of Evaluation Assurance Level 3 (EAL3), 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.

Please refer to Section 9.2 for information on the Canon imageRUNNER ADVANCE Hard Disk Drive Security Kit Options.

* Please see the imageRUNNER Bulletin #5.10 issued on 4/26/10 entitled Hard Disk Drive Format Technology Procedures for imageRUNNER, imageRUNNER ADVANCE and imagePRESS devices to learn more about this feature.

HDD Data Erase Kit

The optional HDD Data Erase Kit 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. Or DoD 5022.22M 3-pass overwrite mode.

Please refer to Section 9.2 for information on the Canon imageRUNNER ADVANCE Hard Disk Drive Security Kit Options.

Timing of Overwrite

The timing of the delete is sensitive to what mode and finishing options are set at the time of print out. Generally, if a jam or other unexpected abnormal end to operation occurs on the device, page data will be stored until the job can be completed and then overwritten on the hard disk drive.
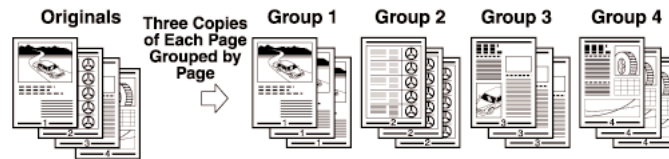
Section 3 – Information Security

Please see below for overwrite examples of what occurs on the device in certain job modes using a job consisting of three sets of three originals.
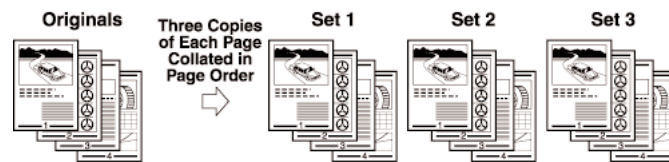
1. Copy/Print Mode:

a. Group Sort
When a user programs a job to be sorted into group sets with no finishing specified, the page data would be overwritten every time a 'set' is complete.
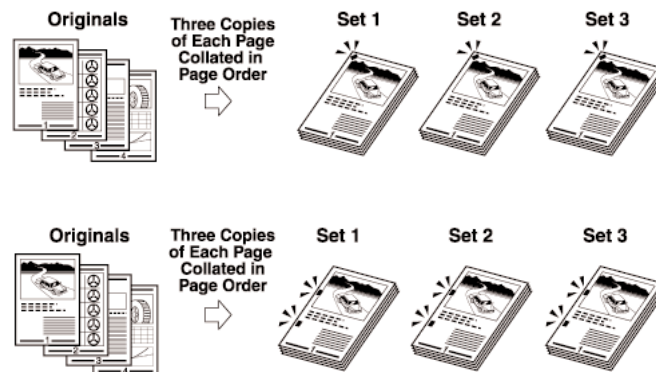

b. Collate Sort
When a user programs a job to be sorted into collated sets with no finishing specified, the page data would be overwritten as each page of the last set is printed out.

c. Staple Sort
When a user programs a job to be sorted into stapled sets, the page data will be overwritten page-by-page after all of the stapled sets finish printing.

d. Remote/Cascade Copy
When a user programs a remote or cascade copy job, depending on the settings chosen, page data will either immediately be overwritten page-by-page or the page data will be overwritten page-by-page after the entire job has finished.

2. Mail Box Print

a. Mail Box Print
When a user prints a job stored in the Mail Box, all pages will be overwritten immediately after the entire job has printed out.

3. Send/Scan Job

a. Send/Scan data
When a user sends or scans a job to another destination, all page data will be deleted or overwritten immediately after the entire job has been sent.

b. Fax/I-Fax Data
When the "Fax Activity Report" function is set to 'On', the data will be overwritten immediately after the device receives confirmation of a successful transmission.
If the failed transmission occurs, the data will remain while the device retries. If the "Fax Activity Report" is set to "off" all data will be deleted at once.

**Performance Impact Using the HDD Data Erase Kit**
It is important to note that the HDD Data Erase Kit settings can affect overall performance of the device depending on what types of jobs are being submitted to the device, and the selected level of overwrite protection. If many large jobs are sent to the device with the 'Overwrite Three Times' option selected, then delays, although minimal, should be expected for devices with speeds over 50 images per minute (ipm). For devices with speeds lower than 50 ipm, HDD Erase Kit related settings will have no impact on performance.

Removable HDD Kit
The imageRUNNER Removable HDD Data Kit option 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.

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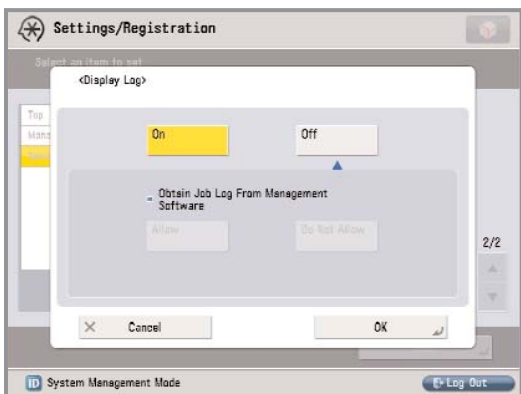
When [On] is selected, the job log is displayed. If Job Log Display is set to [Off], the following features and settings will not be displayed on screen or activated:

- 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].

Job Log Conceal Screen

Section 3 – Information Security

Essentials Workflow Composer
Canon imageRUNNER ADVANCE Essentials includes the Workflow Composer component to enable users and administrators to create custom workflows that automate redundant tasks and provide integration with back-end systems via connectors. Administrators are able to create workflows for users to reduce errors when sending documents and limit access to only designated individuals for operations that interact with back-end systems.

Trusted Platform Module
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.

Data in Transit

Encrypted Secured Print
Encrypted Secured Print utilizes strong AES 256 bit encryption to protect your print job data while in transmission over the network. To protect print jobs from being output at the device unattended, the Encrypted Secured Print feature holds the job in a queue until the user-defined password is entered on the control panel.

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

Section 3 – Information Security

3.3 – 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, but 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.

Fax Polling
Fax Polling is the only function that enables users to handle documents stored in a polling box. Any action associated with these documents stored in a polling box is performed using G3 Fax protocols, which provide no means of accessing a local network.

Other Fax Features

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.

One of the most common means for unauthorized people to gain access to any connected device is through a network, either wired or wireless. Canon provides administrators with a host of powerful controls to limit access to authorized users and devices, enable and disable system services, and ensure the privacy of information sent over networks through strong encryption technologies.

Section 4 – Network Security

4.1 – Network and Print Security (Canon Network Printer Kit Only)

Canon imageRUNNER ADVANCE systems include a number of highly configurable network security features that assist in securing information when the optional Network Print Kit 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:

Name	Port	Description	Setting location	Functions Impacted By This Port
FTP	TCP 21	File Transfer [Control]	Settlings / Registration › Preferences › Network › TCP / IP Settings › FTP Print Settings	If disabled, FTP printing/scanning options will be disabled.
SMTP	TCP 25	Simple Mail Transfer Protocol	Settlings / Registration › Preferences › Function Settings › Send › Email / I-Fax Settings Communication Settings	E-mail and I-Fax sending capability are enabled through this function.
HTTP	TCP 80	World Wide Web HTTP	Settings / Registration › Preferences › Network › TCP / IP Settings › Use HTTP	No access to the imageRUNNER Remote UI utility if disabled. Printing over IPP will cease if disabled.
netbios-ssn	TCP 139	NETBIOS Session Service	Settings / Registration › Preferences › Network › SMB Server Settings › Use SMB	Scanning to a windows folder will be affected.
HTTPS	TCP 443	HTTP protocol over TSL/SSL. Can be used with the following functions:		If enabled, all network traffic between user pc and imageRUNNER device via the Remote UI utility is secure.
		Remote UI	Settings / Registration › Management Settings › License / Other › Remote UI › Select On › Use SSL, Select On or Off	
		MEAP Settings	Settings / Registration › Management Settings › License / Other › MEAP Settings › SSL Settings › Select On or Off	
		IPP Print Settings	Settings / Registration › Preferences › Network › TCP/IP Settings › IPP Print Settings › Select On › Use SSL, Select On or Off	
		Device Information Delivery Settings	Settings / Registration › Management Settings › Device Management › Device Information Delivery Settings › Restrict Receiving for Each Function › Select On or Off	
		Confirm Department ID PIN	Settings / Registration › Preferences › Network › TCP/IP Settings › Confirm Department ID PIN › Select On or Off	
		E-Mail/I-Fax: Authentication/Encryption	Settings / Registration › Function Settings › Send › E-Mail/I-FAX Settings › Communication Settings › Authent./Encryption › Allow SSL (SMTP Receive), Allow SSL (SMTP Send), and Allow SSL (POP)	
PRINTER	TCP 515	Spooler	Settings / Registration › Preferences › Network › Use Spool Function › Select On or Off	Disabling this protocol will cease Printing over LPR.
IPP	TCP 631	IPP (Internet Printing Protocol)	Settings / Registration › Preferences › Network › TCP / IP Settings › IPP Print Settings › Select On or Off	Disabling this protocol will cause Printing over IPP protocol to stop.
HTTP (Meap)	TCP 8000	World Wide Web HTTP for MEAP	Settings / Registration › Management Settings › License / Other › MEAP Settings › SSL Settings › Select On or Off	Disabling this feature disables access to MEAP SMS Page and other MEAP applications such as iWAM for MEAP.
RAW	TCP 9100	Standard TCP/IP Printer (RAW)	Settings / Registration › Preferences › Network › TCP / IP Settings › RAW Print Settings › Select On or Off	Disabling this feature causes Printing over Std TCP/IP protocol to stop.
SNMP	UDP 161	Simple Network Management Protocol	Settings / Registration › Preferences › Network › TCP / IP Settings › SNTP Settings › Select On or Off	Disabling this feature will result in imageRUNNER devices not being discovered or manageable by device management utilities such as iWEMC.

Used ports and default port settings may vary per model. Please consult your device manuals or contact your service technician for additional details.

Section 4 – Network Security

IP Address Filtering

Using the RX/Print Settings function, the System Manager can limit network access to the device to specific IP addresses or ranges for printing and Settings/Browsing. Up to eight individual or consecutive address settings can be specified. Subsequently, the System Manager can also choose to permit a range of addresses, but reject specific addresses within that range.

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.

SSL 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 MFP 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) encryption support for some transmissions to and from the imageRUNNER device, such as Internet protocol Printing (IPP) , Internet-fax (I-fax), Remote UI, Web Access and DIDF.

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 an optional IPSec Board, 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.

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.

See the imageRUNNER ADVANCE system manual for the specific device in question for additional instructions on registering IPSec-based security policies.

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

Wireless LAN
Canon imageRUNNER ADVANCE systems support wireless networking through the installation of an optional Wireless LAN Board. The Wireless LAN Board is IPv6 compliant and supports the latest wireless traffic encryption standards, including WEP, WPA and WPA2, in addition to support for the IEEE802.1X authentication standard.

The Wireless LAN Board and the standard network interface of imageRUNNER ADVANCE systems cannot be used simultaneously, eliminating the possibility of maliciously using the device as a router or bridge to inter-connect two networks. Network communication functionality is automatically disabled for the standard network interface when the Wireless LAN Board is enabled.

Section 4 – Network Security

IEEE 802.1X
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. The Extensible Authentication Protocol (EAP) is attached to both wired and wireless LAN networks, allowing multiple authentication methods such as cards and one-time passwords.

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.

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 for increased security. 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.

USB Block
Administrators have complete control over enabling or disabling access to the imageRUNNER ADVANCE system's USB port, and can independently control the ability to connect to computers or plug-in peripherals.

For more information on the USB Block feature, please refer to the *Device Security* section.

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 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 'TIFF" files received in the e-mail are discarded immediately after reception.
- **Viruses pretending to be TIFF files:**
  TIFF image files are compressed with formats such as MH, MR, and MMR. The imageRUNNER ADVANCE system compresses the '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 '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.

4.2 – Mail Server Security

When the Scan and Send on imageRUNNER ADVANCE devices is enabled, the internal mail service is enabled and supports the POP and SMTP 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.

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.

Section 5 – 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.

5.1 – 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 MFP infrastructure, imageWARE Enterprise Management Console facilitates the secure distribution of device configuration information and address books using SSL encryption, as well as distributing standard and custom driver configurations to client workstations on the network.

5.2 – 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.

For more information on restricting access to the device's setup screens, please refer to the *Device Security* section.

5.3 – 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.

For more information on the Access Management System, please refer to the *Device Security* section.

Section 6 – 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 developed a number of cutting-edge technologies to provide administrators with powerful ways to discourage leaks and investigate unauthorized access.

6.1 – Document Scan Lock & Trace

On imageRUNNER ADVANCE systems, users and administrators can enable the optional Document Scan Lock & Trace feature to place restrictions on the use of hardcopy originals. If a locked document is copied, scanned or faxed on another imageRUNNER ADVANCE system with the document scan lock trace feature installed and enabled, the operation will be locked-out and a record of its unauthorized copying with the user's name will be logged.

The "Lock" capability of the Scan Lock Trace feature needs to be separated from the "Trace" capability and the details listed below need to be added:

LOCK
The available restrictions are as follows:

1. Prohibit All: No one can make any copy/send/fax
2. Password Authentication: Allow to make copy/send/fax only if proper password is entered
3. User Authentication: Allow to make copy/send/fax only to authorized user with proper User ID and Password

TRACE

1. Ability to embed hidden Tracking Information such as User Name, Date/Time and Device Name on the background of the copied and printed document
2. Document Scan Code Analyzer for MEAP allows you to track Who, When and with Which device the document was copied or printed by simply scanning the document on the device
3. Only the authorized personal can access to the tracking information of the document by entering a required password

The Document Scan Code Analyzer for MEAP, which is available only to users in the system administrators group, to track who, when and with which device the document was copied or printed by simply scanning the document containing the hidden tracking code on the device.

For more information on the Document Scan Lock & Trace feature, please refer to the *Document Security* section.

Section 6 – Logging & Auditing

6.2 – Canon imageWARE Accounting Manager

Canon imageWARE Accounting Manager provides enhanced audit tracking capabilities to the end-user environment. In addition to tracking usage by Department ID or SSO account, imageWARE Accounting Manager in conjunction with SSO will provide the ability to track usage per individual user.

Canon imageWARE Accounting Manager provides the capability to:

- Track copy, scan, send & fax jobs.
- Track by paper type, single and double-sided output or N-Up output
- Track by device
- Track by Individual, group or department
- Track by black-and-white or color copy/print jobs
- Multi-tiered billing codes for charge back purposes
- Analyze department/device workload
- Enforce usage limits
- Export reports
- Input billing codes from the device control panel through MEAP application

Canon imageWARE Accounting Manager uses the Department ID of authenticated users to manage and track usage. When SSO authentication is used, administrators can map the user credentials to the respective Active Directory account for tracking.

6.3 – Canon imageRUNNER ADVANCE Tracker

The imageRUNNER ADVANCE Essentials option includes the Tracker feature that provides the ability for users, administrators and other accounting-related departments to monitor, manage, and allocate costs in real-time to prevent inefficient and wasteful usage. Tracker is a server-less solution for cost recovery that can be viewed from the device's control panel, via the web, through automated e-mail reports, or through integration with imageWARE Enterprise Management Console Accounting Manager Plug-In for more in-depth reporting.

6.4 – imageWARE Secure Audit Manager

Canon imageWARE Secure Audit Manager (iWSAM) is an optional robust and efficient information security solution that captures and archives all copy, scan, print, fax and send jobs. When installed, the full image of the document, any embedded images, text, job log, and attribute information such as user name, IP Address, device names, and time/date stamp is indexed and stored for future searching and auditing. In the event that an information breach does occur, iWSAM can be used to help trace the potential source of the leak if it was processed on a Canon MFP. Optional HP printer support is also available.

Section 7 – 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.

7.1 – Common Criteria

Beginning on July 1, 2002, the Department of Defense required a broad group of commercial hardware/software suppliers to have their products evaluated using a standard known as Common Criteria to determine its fitness for the department's use.

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

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

7.2 – Common Criteria Certification

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

Section 7 – Canon Solutions & Regulatory Requirements

7.3 – Authorized Send for CAC/PIV

Designed to meet the needs of the United States Department of Defense and numerous government agencies, the Authorized Send for CAC/PIV option for imageRUNNER ADVANCE systems provides a means for the devices maintain high productivity for walk-up users to output hard copies of the documents they need while restricting access to the Send To features to users who have been authenticated using their Common Access Card (CAC) and/or Personal Identity Verification (PIV) card.

For more information on the Authorized Send for CAC/PIV, please refer to the *Device Security* section.

Section 8 – Conclusion

Since initially introduced, the highly successful Canon imageRUNNER series of devices have rapidly grown in both the breadth and depth of features and functions. With each release, these devices have become increasingly integrated within the IT and network infrastructure. As with any networked device, imaging and printing devices must be included within the broader context of the company's overall security strategy to ensure the confidentiality, integrity and availability of information.

To meet the need for a comprehensive and customizable security solution for any environment, Canon imageRUNNER ADVANCE systems offer a robust set of standard features and optional components. 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.

As corporate privacy goals and regulation guidelines have become stricter, it is important to assess the level of security that all deployed imaging and printing devices provide. After careful review, existing devices may need to be either upgraded or replaced based on each unique environment.

Canon is committed to the security of mission critical information, and is continually developing new technologies to provide a total and reliable solution. For more information, please visit http://www.usa.canon.com.

Section 9 – Addendum

9.1 – 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. 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. 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

Section 9 – Addendum

9.2 – Canon imageRUNNER ADVANCE HDD Security

	Data Encryption & Mirroring Kit-C1	Data Erase Kit-C1
Common Criteria Certification	EAL3	N/A
Supported Devices	iR ADV C5051, C5045, C5035, C5030, C7065, C7055, C9075 PRO, C9065 PRO	iR ADV C5051, C5045, C5035, C5030, C7065, C7055, C9075 PRO, C9065 PRO
Activation	Install Encryption Board	LMS License Access Key
Deactivation	Uninstall the Board	Yes
HDD Encryption	AES (256 Bit)	—
HDD Overwrite	—	X
Overwrite Pattern	—	Null: Once Random Data: Once Random Data: 3 times DoD 5022.22M Compliant Mode
Mail Box Password		
7-Digit Password Required		
Authentication Failure 1 Second UI Lock		
2x Password Entry at Registration		
System Manager Password		
7-Digit Password Required	—	
Authentication Failure 1 Second UI Lock	—	
Password Initialization in Service Mode	—	X
2x Password Entry at Registration	—	
ScanGear Support	X	X
imageWARE® DM Support	X	X
MEAP®	X	X
Web Access Software Support	X	X
Encryption of Attached File on I–FAX	X	X
Displaying the Security Kit Version	X	X

Functions (vertical label)

Legend: X = Feature available   — = Does not apply   N/A = Not available

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

Canon

1-800-OK CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042