Canon

White Paper: Canon imageRUNNER/imagePRESS 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/ imagePRESS series devices. It provides details on Canon's security position 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 Canon MFP devices. The information in this document, in conjunction with other best practices, may be used as guidance to help improve your organizations 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 and imagePRESS devices.

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 the Canon imageRUNNER and imagePRESS product portfolios are designed to help prevent data loss, help protect against unwanted device infiltration and help keep information from being compromised."

> —Dennis Amorosano, Sr. Director
>   Software Product Marketing, Solutions Business Development Division, 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 the imageRUNNER/imagePRESS product portfolio designed to 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/imagePRESS Security White Paper has been designed to provide detailed information on how the imageRUNNER and imagePRESS series of devices can address a wide variety of security concerns. imageRUNNER and imagePRESS devices 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.

Section 2 — Canon's Imaging & Printing Security Framework

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/imagePRESS devices include many standard security features to help safeguard information.

Canon imageRUNNER security capabilities fall into three key areas:

- Device Security
- Network Security
- Security Monotoring/Management Tools

2.1 – Device Security

imageRUNNER/imagePRESS Controller Security

At the heart of every imageRUNNER/imagePRESS device is the Canon imagePlatform controller. The controller runs a proprietary operating system that is not widely available or distributed, and has been expressly designed to run embedded applications developed by Canon. Because of its uniqueness and hardened implementation, the operating system is not a common target for viruses or hackers.

User Authentication Modes

Canon imageRUNNER/imagePRESS devices include a number of authentication options which administrators can use to ensure that only approved walk-up users can access the device and its functions, such as copy, scan and Universal Send features. Beyond limiting access to only authorized users, authentication also provides the ability to control usage of color and black and white output, and total print counts by department or user.

The user authentication methods that imageRUNNER/imagePRESS devices support include:

- Department ID
- Simple Device Login (SDL)
- Single Sign On (SSO)

Department ID Mode

An embedded feature within the imageRUNNER/imagePRESS devices, 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.

Each Department ID can be configured with device function limitations, such as the maximum number of copies, copy and Mail Box allocation parameters, size of Mail Box and facsimile access. The total number of Department IDs that can be defined on each device depends on the specific imageRUNNER/imagePRESS model. Customers can also add an optional card reader unit to enhance security by providing authorized users with control cards to access the machine.

Mail Box, Send (if applicable), and Scan functions can each be turned "On" or "Off" from the Limit Functions screen located under Department ID Management. Copy mode, is automatically disabled when the Department ID Management function is turned "On". Once a mode has been turned "On" (deeming it password-protected), the tab for that mode will be grayed-out on the LCD panel.

The settings can be made under ⊚ Additional Functions → System Settings → Department ID Management → Store Dept. ID/Password → Limit Functions.

Section 2 — Canon's Imaging & Printing Security Framework

Simple Device Login (SDL)
Simple Device Login is a MEAP login service that can be used stand-alone with the device. User data is registered in the device's memory using a web browser.

The SDL login service provides the following functions:

- Displays a login screen on the touch panel display of the device, and performs user authentication
- Displays a login page when the device is accessed from a web browser, and performs authentication
- Enables you to limit and keep track of the print/scan totals for department IP, by linking to the department ID Management functions of the device

The SDL login service can be configured using the MEAP Service Management Service.

To enable the SDL login Service, open a web browser and enter the URL http://<imageRUNNER IP Address or host name>:8000/sms. On the login page type the password. Click on the System Management tab. Click on the Enhanced Sys. App tab.Under login service select "Simple Device Login." Click the select button. Reboot the device.

Single Sign On Login
Single Sign On (SSO) is a MEAP login service that can be used in conjunction with an Active Directory (AD) network environment. SSO supports the following modes:

- Local Device Authentication
- 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 Windows AD credentials prior to gaining access the any of the MFP device functions.

SSO ships standard with MEAP capable imageRUNNER and imagePRESS devices and can support up to 200 domains. The latest device models ship with a version of SSO called SSO-H, which supports direct authentication against AD using Kerberos or NTLMv2 as the authentication protocol. In local device authentication, SSO-H can support up to 5,000 users.

Earlier MEAP devices support a version of SSO that utilizes a Security Agent (SA) to accomplish authentication against AD. The SA is a small Windows application which can be run on any PC system that is a member of the same Windows domain. This earlier version of SSO only supports NTLMv2 as the authentication protocol and can support up to 1,000 users.

To enable the SSO login Service, open a web browser and enter the URL http://<imageRUNNER IP Address or host name>:8000/sms. On the login page type the password. Click on the System Management tab. Click on the Enhanced Sys. App tab. Under login service select "Single Sign-On." Click the Select button. Reboot the device

Section 2 — Canon's Imaging & Printing Security Framework

Advanced Access Control*

Canon imageRUNNER/imagePRESS devices support a number of advanced access control options to help you manage their use and restrict unauthorized users. These options provide a range of features to help manage Authentication, Authorization, and Auditing.

Authentication options include support for proximity cards, PIN codes as well as smart cards. In the area of Authorization, Canon offers solutions that can lock down the entire device, or simply lock down specific functions (ex. Send-to-Email), while leaving other applications available for general use. These solutions can log activity like copying, printing, faxing, scanning, and email, to provide you with the Auditing information you need to track usage down to the individual user level.

With the power and flexibility of MEAP, many of these authentication solutions can be customized to meet your specific requirements.

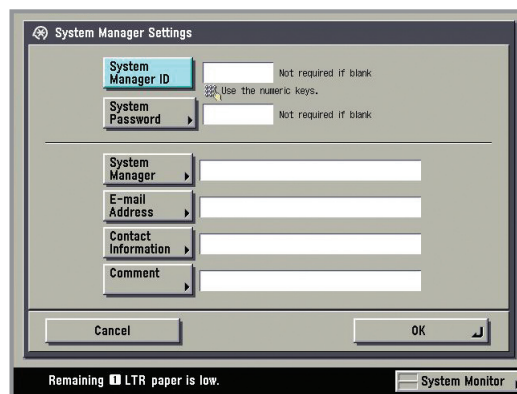**Control Cards/Card Reader System***

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

Password-Protected System Settings

As a standard feature, imageRUNNER/imagePRESS device setup screens support password protection to restrict device setting changes from the control panel and Remote UI tool. When a device administrator uses the System Settings menu, they 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.
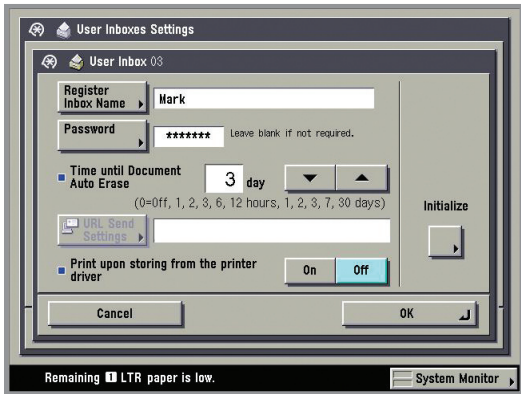
System Manager Screen   Store ID and Password Screen

Not available on all imageRUNNER/imagePRESS models.

Section 2 — Canon's Imaging & Printing Security Framework

Box Set/Store Password Screen

Mail Box Password Protection
Each imageRUNNER/imagePRESS product ships standard with support for up to 100 Mail Boxes for storage of scanned and printed data. Mail Box security is provided by the ability to designate a unique passwords for access.

HDD and RAM Data Protection
Canon imageRUNNER/imagePRESS devices, like many other multifunction devices, use a combination of Random Access Memory (RAM) and an internal Hard Disk Drive (HDD) for short-term and long-term data storage when handling system functions like copying, printing, and faxing. The internal HDD, as used by the imagePlatform controller, is formatted with two partitions — Partition A and Partition B.

Partition A, which is used to store spooled print jobs, is formatted with a FAT16-like file system that is not accessible from DOS/Windows. The print jobs stored on Partition A are automatically deleted at the following points:

- After they are rendered to image files in memory
- When a device has not successfully received a job
- When a job is canceled by a user's operation
- When the machine's power is turned on, if any files remain

Partition B is formatted with a Canon proprietary file system, which is not compatible with any commonly used file system. All image data is written to Partition B in random and non-contiguous portions of the hard disk drive, making it difficult to meaningfully analyze or reassemble data.

To properly recompile this randomly written data, it is necessary to store the location and sequence of all data written to the HDD. The imagePlatform controller accomplishes this by creating a File Allocation Table (FAT) that stores all appropriate data locations and sequence on the HDD. Upon finishing a specific job, whether it is printing, copying, or faxing, the system automatically erases the FAT. As a result, all information required to recompile data in the image server is lost.

Although the reference to deleted files has been removed from the FAT, the actual data may remain on the HDD or RAM until overwritten by subsequent jobs. As a result data could still be compromised, although doing so would be extremely difficult.

For customers who may be concerned about residual data on hard drives, Canon recommends the use of the optional HDD Data Erase Kit.

MEAP Security
Canon actively collaborates with leading third-party software companies to develop extensible solutions for the imageRUNNER/imagePRESS devices, known as MEAP applications. Each MEAP enabled device includes a number of safeguards to 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's integrity is guaranteed by Canon and is digitally signed with a special encrypted signature and license for protection purposes. 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/imagePRESS device.

Section 2 — Canon's Imaging & Printing Security Framework

2.2 – Network Security

Network and Print Security (Canon Network Printer Kit Only)
Canon imageRUNNER/imagePRESS devices 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.

The imageRUNNER/imagePRESS devices 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 (*1)	TCP 21	File Transfer [Control]	System Settings›Network Settings›TCP/IP Settings›FTP Print Settings	If disabled, FTP printing/scanning options will be disabled
SMTP	TCP 25	Simple Mail Transfer Protocol	System Settings›Network Settings›Email/Ifax	E-mail and i-Fax sending capability are enabled through this function
HTTP	TCP 80	World Wide Web HTTP	System Settings›Network Settings›TCP/IP Settings›Use HTTP	No access to the imageRUNNER's Remote UI utility if disabled. Printing over IPP will cease if disabled.
netbios-ssn	TCP 139	NETBIOS Session Service	System Settings›Network Settings›SMB Settings›Use SMB	Scanning to a windows folder will be affected.
HTTPS	TCP 443	HTTP protocol over TLS/SSL	System Settings›Network Settings›TCP/IP Settings› press [On] for ‹Use SSL›.	If enabled, all network traffic between user pc and imageRUNNER device via the Remote UI utility is secure.
PRINTER	TCP 515	spooler	System Settings›Network Settings›Use Spooler› press [On]	Disabling this protocol will cease Printing over LPR
IPP	TCP 631	IPP (Internet Printing Protocol)	System Settings›Network Settings› TCP/IP Settings screen› press [IPP Print Settings]› press [On]	Disabling this protocol will cause Printing over IPP protocol to stop.
HTTP	TCP 8000	World Wide Web HTTP for MEAP	System Settings› MEAP Settings› Set [Use HTTP] to [On]	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)	In the printer properties dialog box, click [Configure Port] ›select [LPR] or [Raw].	Disabling this feature causes Printing over Std TCP/IP protocol to stop
SNMP	UDP 161	Simple Network Management Protocol	System Settings›Network Settings›TCP/IP Settings› [SNTP Settings]› [On] for [Use SNTP]	Disabling this feature will result in imageRUNNER devices not being discovered by device management utilities such as iWEMC or Netspot Device Installer

* Used ports and default port settings may vary per model. Please consult your device manuals or contact your service technician for additional details.
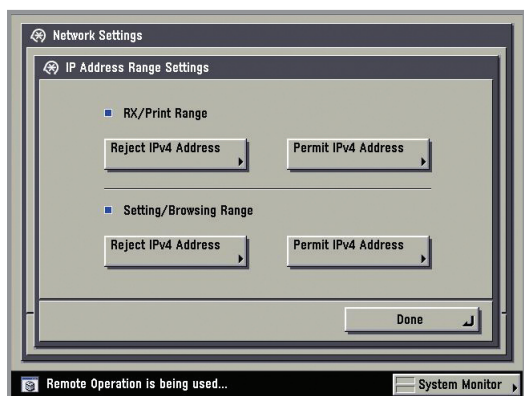
IP Address Range Settings Screen

IP Address Range Settings

Using the RX/Print Settings function, the System Manager can limit network access to the device to specific IP addresses or ranges for printing. 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.

Unless an address has been restricted by the RX/Print Settings function, the Setting/Browsing Range feature will permit all users to print from their PCs. However, this setting can also alter whetherspecific users can use Remote UI functionality or not. **To block access to the Remote UI utility, System Managers simply need to go to Network Settings → TCP/IP Settings → IP Address Range Settings → Setting/Browsing Range and enter in the IP address of the devices they wish to block. Like the RX/Print Settings, the System Manager can set a total of eight settings of either individual addresses or ranges.**

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.

IPv6 Support

IPv6 support is available in all newly released imageRUNNER/imagePRESS models, and available through a firmware upgrade for some older devices. IPv6 provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4. The United States Department of Defense (DOD) has established the goal of transitioning all their networked devices to the next generation of IPv6 by Fiscal Year 2008. Other agencies government-wide are beginning to move towards this trend and require IPv6 for all networked devices.

IPsec Support*

The latest imageRUNNER/imagePRESS devices support an optional IPSec Board, which allows users to utilize IPSec (Internet Protocol Security) to 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.

Once you install the optional IPSec Board to the device, you can use IPSec communications by going to Network Settings → TCP/IP Settings → IPSec Settings and set ‹Use IPSec› to [On]. ([IPSec Settings] is only displayed on the TCP/IP Settings screen if the optional IPSec Board is installed on the device). See the imageRUNNER/imagePRESS manual for the specific device in question for additional instructions on registering IPSec-based security policies.

Not available on all imageRUNNER/imagePRESS models.

Section 2 — Canon's Imaging & Printing Security Framework

Authentication and Encryption Method:

At least one of the following methods must be set for the device. You cannot set both methods at the same time.

- 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
The latest imageRUNNER devices can also 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 the IEEE802.1X authentication standard.

The Wireless LAN Board and the standard network interface of imageRUNNER devices 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.

IEEE 802.1X

The latest imageRUNNER/imagePRESS devices support IEEE 802.1x, which is a standard protocol for port-based Network Access Control and it provides authentication to devices attached to a LAN port. It establishes a point-to-point connection or prevents access from that port if authentication fails.

It attaches the Extensible Authentication Protocol (EAP) to both wired and wireless LAN networks for allowing multiple authentication methods like cards and one-time passwords.

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

IEEE 802.1x addresses the following IEEE 802.11 security issues:
- • User Identification & Strong authentication
- • Dynamic key derivation
- • Mutual authentication
- • Per-packet authentication
- • Dictionary attack precautions

Printer Driver Security Features

Secured Print/Encrypted Secured Print

Encrypted Secured Print and Secured Print are authenticated 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/imagePRESS device 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 Secure Print job data while in transit across the network. On imageRUNNER/imagePRESS Series devices equipped with the optional encrypted secured print, administrators can use the print job restriction feature to permit only encrypted secured print jobs at the designated imageRUNNER/imagePRESS device.

Administrators can force all users to utilize encrypted secured print* using the following settings: Press ⊙ Additional Functions → System Settings → Only Allow Encrypted Secured Print Jobs → Set to [On]. A job will be canceled and an error message displayed if a print job other than an encrypted secured print job is received. (The default setting is [Off].)
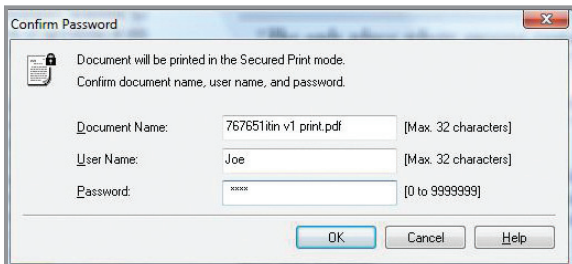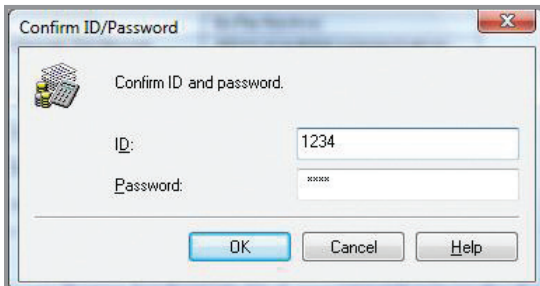
Secure Print Screen from the Printer Driver
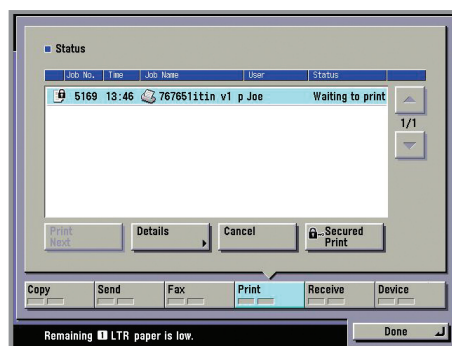
Print Job Status Screen

* When imageRUNNER/imagePRESS device is equipped with optional encrypted secured print software.

Section 2 — Canon's Imaging & Printing Security Framework


Print Job Accounting Screen

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.

Mail Box Printing

Another secure document delivery feature, Mail Box printing allows users to send a job to their individual Mail Box. Once stored in the Mail Box (if the Mail Box is password protected), a user must enter their password to retrieve documents. On newer imageRUNNER/imagePRESS devices, administrators can use the Print Job Restriction feature to restrict direct printing from a desktop to the Color imageRUNNER/imagePRESS Series. This forces all print jobs to be stored in a Mail Box or in the Hold Queue before printing can be performed by users.

Administrators can force all users to utilize Mail Box printing using the following settings: Press ⊙ Additional Functions → System Settings → Restrict Printer Jobs → Set to [On] (The default setting is [Off]). A job will be canceled and an error message displayed if a print job other than a store to user inbox print job is selected as the output method.
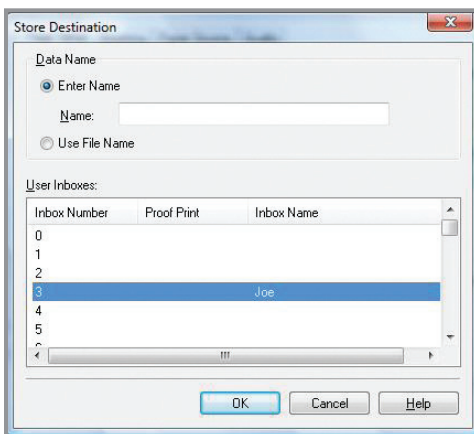
Mail Box Store Destination Screen

Mail Box Set/Store Password Screen

Universal Send Security

For Universal Send enabled devices, information found in the Send screen may be considered confidential and sensitive to certain users. For these devices, there are additional security features to prevent confidential information from being released. All new imagePlatform based devices have a System Settings button that can be protected by a System Manager ID and System Password to prohibit anyone other than the System Manager from changing device settings.

The Universal Send Security Feature Set enables you to encrypt PDF files and set a password to send PDF files safely to a file server or e-mail address. It also enables the recipient of the PDF or XPS files to verify which device scanned it.

Encrypted PDF:

The Encrypted PDF mode enables you to encrypt PDF files that you send 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.

Device Signature PDF or Device Signature XPS*:

The Device Signature PDF or the Device Signature XPS mode uses the device signature certificate and key pair inside the machine to add a digital signature to the document, which enables the recipient to verify which device scanned it.

User Signature PDF or User Signature XPS:

If the optional Digital User Signature PDF kit is activated, users can install a digital signature that embeds their name and email address to confirm their identity as the source of the document and notification if changes have been made. In order to use Digital User Signature Mode, SDL or SSO authentication must be enabled and a valid certificate installed on the device.
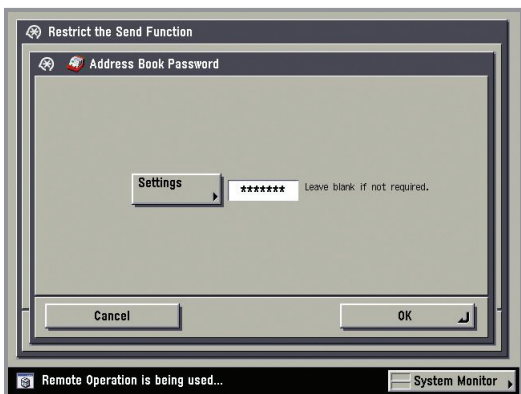
Address Book Password Screen

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 from the System Settings user name and password, 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 book is restricted. Therefore, only individuals with the correct password for an Address Book will be able to make modifications. System Managers can set the password in Additional Functions → System Settings → Restrict the Send Function → Address book Password. A maximum number of seven digits may be set as the password.

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

Not available on all imageRUNNER/imagePRESS models.

Section 2 — Canon's Imaging & Printing Security Framework
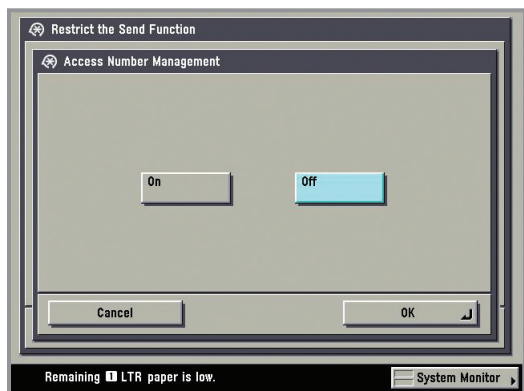
Address Book Access Code Enable/Disable Screen

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 in the Additional Functions section, users can then enter an Access Number to restrict the display of that address in the book. This function limits the display and use of an address in the Address Book to those users who have the correct code. The Access Number can be turned on or off, depending on the level of security the end-user finds necessary. **The Access Number can be set in Additional Functions → System Settings → Restrict the Send Function →Access Number Management.**

Destination Restriction Function
Data transmission to a new destination with Universal Send can be limited through the use of System Settings. This function prohibits 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 Universal Send. 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 SDL/SSO login)

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/imagePRESS 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.

imageRUNNER/imagePRESS devices use "private" and "public" as the default SNMP community strings, but these may be renamed to a user-defined value for increased security.

To modify SNMP community strings go to Additional Functions → System settings → Network Settings → SNMP Settings.

USB Block

USB Block allows the System Administrator to help protect the imageRUNNER/imagePRESS device against unauthorized access through the built-in USB interface. Access to the imageRUNNER/imagePRESS through the USB interface for desktop access and the device's host mode for other USB devices can each be permitted or disabled.

Go to Additional Functions → System settings → USB Settings → Use USB Device On/Off or → Use USB Host On/Off.

Virus Concerns for Email Reception

For those imageRUNNER / imagePRESS devices with Universal Send capabilities, if an e-mail with an attached data virus is received, the imageRUNNER/imagePRESS will always discard the virus upon receipt.

Universal 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:

1. 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.

2. Viruses pretending to be TIFF files:
TIFF image files are compressed with formats such as MH, MR, and MMR. The imageRUNNER/imagePRESS device 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.

3. 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 (function calls such as fgets() or fprintf()). 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.

Job Log Data Protection

The job history stored within the imageRUNNER/imagePRESS job log may be considered sensitive information by some users. The display of the job log data can be turned ON/OFF. The default of the job log data display is ON.

See page 24 for more information on how to conceal Job Log data.

Section 2 — Canon's Imaging & Printing Security Framework

Fax Security*

Canon imageRUNNER devices 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 in the following manner:

- 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.

- 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 imagePlatform device via its phone line connection cannot be processed.

- 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. 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.

- 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 fax format, there is no threat of virus infection.

- 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 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.

imagePRESS devices do not support fax functionality.

2.3 – 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/imagePRESS device is deployed, or a fleet of imageRUNNER/imagePRESS devices, the imageWARE Accounting Manager and Access Management System software options provide the ability to audit usage and limit access to features and functions enterprise-wide — at the group and user-level.

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 SDL, 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.

*Canon imageWARE Accounting Manager is supported by all imageRUNNER devices and the imagePRESS-C1 model only.

Section 2 — Canon's Imaging & Printing Security Framework

Access Management System Kit*

The Access Management System Kit 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.

The following describes the various base access levels (roles) that are available:

Access Privileges by Access Level	
Access Level	Access privileges
Administrators	Given privileges to operate all device functions
Power Users	Given privileges to operate device functions in user mode and their jobs
Generic Users	Given privileges to operate device functions in user mode except for Address Book and their jobs
Limited Users	Given privileges to operate their jobs only
Guest	Disallowed to modify device settings and denied access to the send, web access, and MEAP functions

Canon Access Management System is supported by all imageRUNNER Devices and the imagePRESS-C1 only.

Section 2 — Canon's Imaging & Printing Security Framework

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	Allowed, Not Allowed	Allows or prohibits using applications related to the Send function. (Including the Fax function).
Mail Box	Allowed, Not Allowed	Allows or prohibits using applications related to the Mail Box function. (Including Job Hold function).
Web Access	Allowed, Not Allowed	Allows or prohibits using application related to the Web Access function.
Utility	Allowed, Not Allowed	Allows or prohibits using applications related to Utilities.
MEAP Applications	Allowed, Not Allowed	Allows or prohibits the use of MEAP applications.
Others	Allowed, Not Allowed	Allows or prohibits using other applications.

Access Management System Realtime Workflow
When the Access Management System has been enabled, users must log in to the device using SDL/SSO user authentication. Access Management System supports authentication through 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, the tab will not appear on the control panel for that particular user or group.

Section 3 — Advanced Security Features

In addition to the wide variety of device and network security features that are standard on imagePlatform-based devices, Canon offers advanced security options to assist companies in meeting their internal privacy goals and address strict regulation guidelines.

Developed in accordance with extended security requirements of key customers and U.S. government agencies, Canon offers advanced security features that include:

- Canon Advanced imageRUNNER Security Solutions
  - HDD Data Encryption
  - HDD Data Erase
  - Job Log Conceal

- Other Optional Advanced Security Features
  - HDD Format
  - Removable HDD

3.1 – Canon Advanced imageRUNNER Security Solutions

HDD Data Encryption Kit
The HDD Data Encryption Kit option ensures that all data stored on the internal disk drive is protected using industry-standard algorithms. The HDD Data Encryption Kit is a dedicated plug-in board that encrypts every byte of data before it is committed to the disk using 256-bit AES (Advanced Encryption Standard) or 168-bit 3DES (Triple Data Encryption Standard) algorithms, depending on the device model.

Encryption on the hard drive is achieved through a multi-step process to mitigate the risk of unauthorized disclosure. First, the imageRUNNER/imagePRESS device uses mathematical algorithms to scramble bits of data. The data is then encrypted using a secret key created in the imageRUNNER/imagePRESS device before it is written to the internal disk drive, providing protection for both temporary and permanent data such as documents stored in Mail Boxes. Finally, the data is stored in random, non-contiguous locations on the imageRUNNER/imagePRESS device's hard drive to make the intelligible reconstruction of files infeasible in the event the disk is removed.

Canon's HDD Data Encryption Kit for imageRUNNER/imagePRESS devices have received Common Criteria Certification of Evaluation Assurance Level 3 (EAL3).

Please refer to the Addendum for information on the optional HDD Data Encryption Kit available for each imageRUNNER/imagePRESS device.

HDD Data Erase Kit
Through the use of the optional HDD Data Erase Kit, security conscious customers can configure their imageRUNNER/imagePRESS systems to overwrite the internal image server hard disk, erasing previous data stored as part of routine job processing. The HDD Data Erase Kit offers administrative options that allow the system administrators to configure the level of overwrite protection.

Section 3 — Advanced Security Features

The following are supported methods of hard drive data erase. Configuration of this setting is made in service mode, by an Authorized Canon Service Technician.

Number of Overwrites	Values	Description
0	OFF	Do not erase (default Setting)
1	ON	Cleared once with NULL data (Clear with "o")
2	ON	Cleared once with random data
3	ON	Cleared three times with random data

A disk overwrite can also be forced by the device administrator through the System Settings option. From Additional function screen, the administrator can select [On] or [Off] for Hard Disk Data Complete Erase. **The settings can be made under ◉ Additional Functions → System Settings → Hard Disk Data Erase.** If [On] is selected, data from the hard disk will be erased completely. If [Off] is selected the data will not be completely erased. The default setting is [Off].

Please refer to the Addendum for information on the optional HDD Data Erase Kit available for each imageRUNNER/imagePRESS device.

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.

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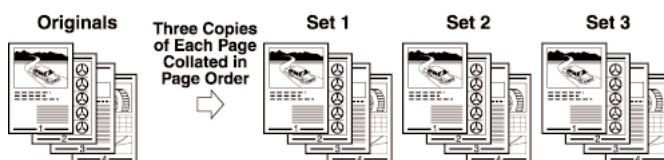
1. Copy/Print Mode:

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.
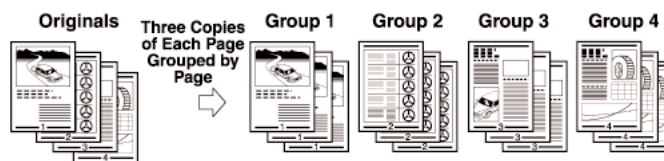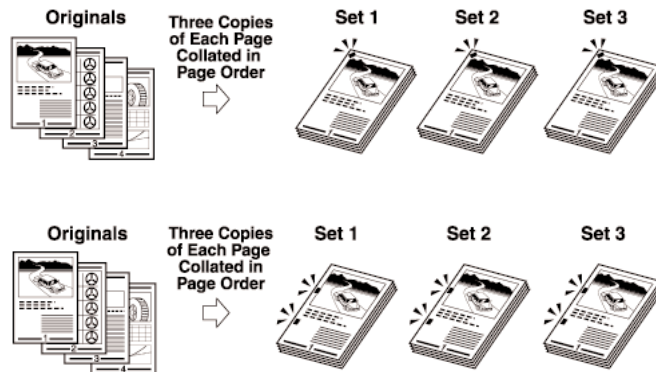

b. Collate Sort
When a user programs a job to be sorted into collated sets with no finishing specified, the page data would be overwritten as each page of the last set is printed out.

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.
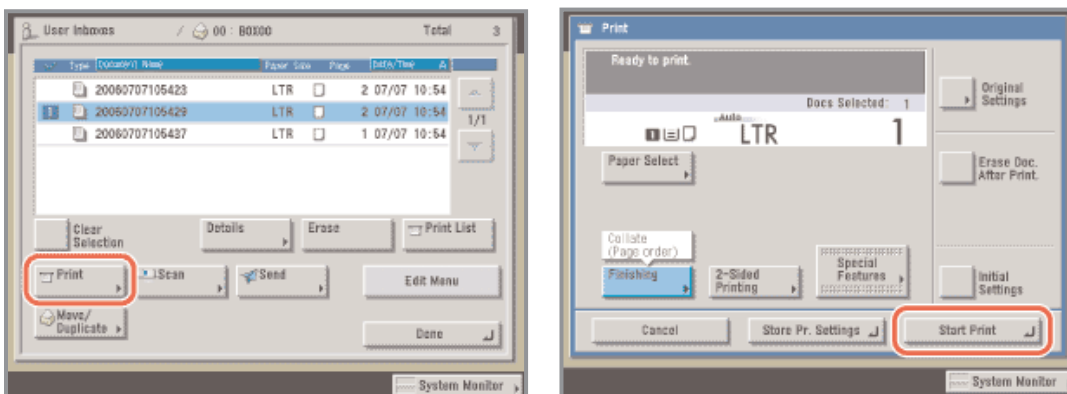
Mail Box Print

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 Erase Kit
It is important to note that the HDD 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.
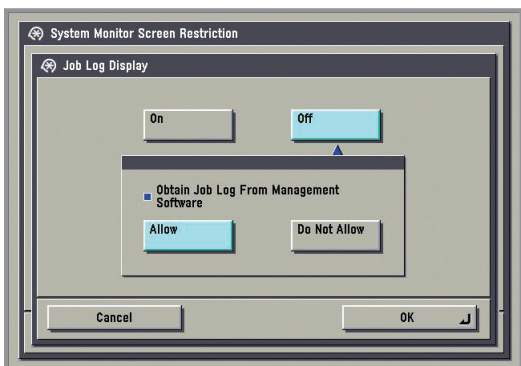
Job Log Conceal Screen

Job Log Conceal Function*
The 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 the Job Log Display under ⊙ Additional Functions → System Settings → System Monitor Screen Restriction → Job Log Display.** 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 Universal 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].

The Job Log Conceal feature is now standard on some newer imageRUNNER models, and available through a firmware upgrade for Color imageRUNNER C5180/C4580/C4080/C3380/C2880 and imageRUNNER 7105/7095/7086/5075/5065/5055 devices.

Section 3 — Advanced Security Features

3.2 – Other Advanced Security Features

Standard HDD Format*
Best practices, and often company policies, usually recommend that systems be completely wiped prior to being redeployed or at the end of its usable life. The Hard Disk Drive Format feature, which is standard with all imageRUNNER/imagePRESS devices, completely overwrites all data stored on the hard disk with null data. This includes files, job logs, Address Books, and customized user mode settings, all in a single operation. If the optional HDD Erase Kit is installed, the HDD Format feature provides additional overwrite options, including the choice to overwrite three times with random data.

Removable HDD**
The imageRUNNER Removable HDD 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.

Section 4 — Security Solutions in non-imagePlatform Devices

This section provides an overview of the security features on non-imagePlatform-based imageRUNNER devices. Due to the difference in architecture from the imagePlatform, non-imagePlatform imageRUNNER devices deal with data differently across certain functions. Whereas the imagePlatform device uses the internal image server memory (RAM or HDD) for copying, printing, and faxing (depending on the model), non-imagePlatform devices use their internal image server memory only for copy and printing functions.

Canon's legacy GP200 Series product line, imageRUNNER 200L, and imageRUNNER 210 lack an image server, therefore the copy function does not store the information on the system. These systems instead make copies on a page-by-page basis, scanning each page based on the number of copies requested. As a result, no page data is stored on the system, which renders it impossible for anyone to walk up to the device and get latent image information. When printing, these devices are unable to store data on the device due to a lack of internal memory and jobs are printed immediately.

4.1 – Standard Device Security

Department ID Management***
An embedded feature in non-imagePlatform devices, this function is used to set parameters for users of the device and the device administrator can set controls that could limit users to a set number of copies, maximum Mail Box allocation and maximum limits for copy/Mail Box functions. As an option, customers can add a card reader unit to the device and control copy maximums based on the configuration of the device.

*Please see the imageRUNNER Bulletin #5.08- HDD Overwrite Procedures for End of imageRUNNER Lifecycle Procedures to learn more about this feature.
**Removable HDD Kit is only available for select imageRUNNER/imagePRESS devices.
***Department ID Management limit function is only available on imagePlatform-based devices.

Restricting Device Setup Screens (displayed on the LCD panel User Interface)
A standard feature, imageRUNNER device setup screens can be password protected, thereby ensuring that administrative device settings are not changed without appropriate authority. When a device administrator uses the System Settings menu, they can set network information, system configuration and enable and disable network and printing protocols among many other options.

Mail Box Password Protection*
The imageRUNNER 550/600/60 and 330/400 product ships with up to 100 User Mail Boxes. These Mail Boxes can be used for storage of scanned and printed data for integrating scanned and printed data, or for up to three days document storage. Mail Box security is provided by the ability to designate unique passwords for access of individual device Mail Boxes.

4.2 – Network and Print Security

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.

Mail Box Printing**
Another secure document delivery feature, Mail Box printing allows users to send a job to their individual Mail Box. Once stored in the Mail Box (if the Mail Box is password protected), a user must enter their password to retrieve jobs previously stored.

4.3 – Memory Security

The majority of jobs processed by non-imagePlatform systems result in images being written to the image server, hard disk drive and RAM, where it is compressed and randomly stored. The FAT (File Allocation Table), which has all the allocation data of the job, is stored in a separate location of the image server. When utilizing their internal image server, the data flow for the non-imagePlatform imageRUNNER products — whether it is RAM (iR330/400) or hard disk (iR550/600) — is directed in the same manner as that of the imagePlatform-based imageRUNNERs.

4.4 – Fax Security

Fax functions on the imageRUNNER200L/210/330/400 will operate in a manner similar to that described under "Fax Security" in Section 2, page 17. Instead of storing page data in an image server, all fax data is stored in RAM on the imageRUNNER 200L/210/330/400 fax board. Other than this, the operation of fax is identical.

Please see Section 2 for more detailed information.

*The Multi-PDL Network printer board or the Network Printer Board needs to be installed in order to use the Mail Box feature.
  Mail Boxes are not available on GP series, imageRUNNER 200L, and imageRUNNER 210 models.
**Does not apply to the GP series, imageRUNNER 200L, and 210.

Section 5 — Canon Solutions and Regulatory Requirements

5.1 – 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.

5.2 – 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 6 — Conclusion

Since initially introduced, the highly successful Canon imageRUNNER/imagePRESS 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/imagePRESS devices offer a robust set of standard features and optional components. When properly deployed, an imageRUNNER/imagePRESS device can be effectively protected against vulnerabilities from either malicious or unintentional use. Combined with advanced monitoring and management tools for auditing and centralized administration, Canon imageRUNNER/imagePRESS devices 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 7 — Addendum

7.1 – Canon Security Recommendations Quick Reference

The following actions are recommended by Canon as appropriate first steps in securing the Canon imageRUNNER or imagePRESS device 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. Set the system administrator ID and password
2. Disable unused ports and applications (e.g. FTP, RUI)
3. Set passwords for MailBoxes
4. Restrict printing and RUI access to specific IP or MAC addresses
5. Set passwords for Address Book management
6. Change the SNMP community strings
7. Disable the USB port if unused
8. Utilize Optional Hard Disk Drive Erase Kit or Hard Disk Drive Encryption Kit to ensure integrity of data stored on internal imageRUNNER/imagePRESS Hard Disk Drives
9. Enable and configure Department ID to manage user device access permissions on a departmental or user level
10. Monitor the devices using imageWARE EMC

7.2 – Compatibility Charts for Optional Hard Disk Drive Data Erase Kits and Encryption Kits

Security kits with separated encryption and data overwrite functions

	Data Encryption Kit	Data Erase Kit
Common Criteria Certification	EAL3	N/A
Supported Devices	Color imageRUNNER C5185/C5185i/ C4580 V2/C4580i V2/C4080 V2/C4080i V2/C3480/C3480i/C3380 V2/C3380i V2/ C3080/C3080i/C2880 V2/C2880i V2/C2550imageRUNNER 7105 V2/7095 V2/7086 V2/7095 PrinterV2/5075/5065/ 5055/3245/3245i/3235/3235i/3230/3225/30 45/3035/3030/3025 imagePRESS C1	Color imageRUNNER C5185/C5185i/C4580 V2/C4580i V2/C4080 V2/C4080i V2/C3480/C3480i/C3380 V2/C3380i V2/ C3080/C3080i/C2880 V2/C2880i V2/C2550 imageRUNNER 7105 V2/7095 V2/7086 V2/7095 PrinterV2/5075/5065/ 5055/3245/3245i/3235/3235i/3230/3225/ 3045/3035/3030/3025 imagePRESS C1
Activation	Install Encryption Board	LMS License Access Key
Deactivation	Uninstall the Board	N/A
HDD Encryption	X (256 Bit, AES)	N/A
HDD Overwrite	–	X
Overwrite Pattern	–	Null: Once Random Data: Once Random Data: 3 Times
Mail Box Password		
7-Digit Password Required		X (Local UI Remote UI)
Authentication Failure 1 Second UI Lock		X (Local UI Remote UI)
2x Password Entry at Registration		X
System Manager Password		
7-Digit Password Required	–	X (Local UI Remote UI)
1 Second UI Lock Authentication Failure	–	X (Local UI Remote UI)
Password Initialization in Service Mode	–	–
2x Password Entry at Registration	–	X
ScanGear Support	X	N/A
imageWARE® DM Support	X	N/A
MEAP®	X	X
Web Access Software Support	X	X
Encryption of Attached File on I–FAX	X	
Displaying the Security Kit Version	Displayed in Device Configuration Screen	

Functions (row label for the function section)

Security kits with both encryption and data overwrite functions

	Security Kit-A Series	Security Kit-B Series
Common Criteria Certification	N/A	EAL3
Supported Devices	imageRUNNER 4570/3570/2870/2270/ 6570/5570/5070/105+/9070/8070/85+/ C3170U/C3170i/7105/ 7095/7095 Printer/7086/C5180/C5185i/C4580/ C4580i/C4080/C4080i/3300i/3300/2800 /2200/3320i/3320N/2220i/2220N/5000i/ 5000/6000/5020/6020/C6870U/C6800/ C5870U/C5800/C3200/C3220/C2620	imageRUNNER 6570/5570/4570/3570/3300/2870/ 2800/2270/2200 (imageRUNNER 5070 is not supported)
Activation	LMS License Access Key	
Deactivation	X (in the Service Mode)	N/A
HDD Encryption	X (168 Bit, TDEA)	X (168 Bit, TDEA)
HDD Overwrite	X	X
Overwrite Pattern	–	Null: Once Random Data: Once Random Data: 3 Times
Mail Box Password		
7-Digit Password Required		X (Local UI Remote UI)
Authentication Failure 1 Second UI Lock		X (Local UI Remote UI)
2x Password Entry at Registration		X
System Manager Password		
7-Digit Password Required	–	X (Local UI Remote UI)
1 Second UI Lock Authentication Failure	–	X (Local UI Remote UI)
Password Initialization in Service Mode	X	–
2x Password Entry at Registration	–	X
ScanGear Support	X	N/A
imageWARE® DM Support	X	N/A
MEAP®	X	X
Web Access Software Support	X	X
Encryption of Attached File on I–FAX	–	X
Displaying the Security Kit Version	–	Displayed in Device Configuration Screen

Functions (row label for the function section)

X = Feature available   – = Does not apply   N/A = Not available

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

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

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