Canon

Canon Security Solutions
for the imageRUNNER® Series

Security offerings that help maximize your organization's ability to deter information theft and fraud

The information contained in this document pertains to Canon's imageCHIP architected devices, known as the imageRUNNER® line of digital multifunctional products. The information in this document is exclusive of imageRUNNER devices capable of speeds of 20 ppm and below.

Your business produces, analyzes and processes information daily. Information is a company's most valuable asset and also the most vulnerable one. Information can be shaped into multiple forms: bits and bytes for network transfer and storage, printed documents, or materials for presentation. Because information can be presented in multiple ways and is found in various locations, it is extremely vulnerable to attacks including data corruption, theft, piracy and destruction.

Most of today's enterprises have built a strong perimeter of firewalls, intrusion prevention systems, and anti-virus software to protect their digital assets. Attention is given to servers, network equipment, and user workstations, but networked printers and multifunctional digital copier devices have been largely ignored when it comes to security. With the advent of the MultiFunctional Printer (MFP), more and more functionalities have been integrated into one system, including scanning, copying, faxing, printing, and even Web access. These devices have become new targets for attackers, as they act as "information hubs," where data from various business units, departments, and users is processed, stored, and produced.

As networked printers and multifunctional systems complete the transformation from output terminal to true network node, businesses and IT professionals need to be just as concerned with data residing on – and passing through – MFP hard drives as they are with PC and network security.

Thus, corporate IT and security departments must include MFP devices as critical assets that require protection from internal and external threats. However, the knowledge needed to protect an MFP is much different than that needed to secure other types of network devices, such as file servers, databases, or routers. Many MFP devices run operating systems and offer hard disk drives to temporarily or permanently store data.

If information theft or virus insertion is the goal, it may be easier and faster to penetrate a single MFP shared by an entire department than to target scores of individual computers. Internal security breaches of intellectual property and confidential information can be as damaging to your business as the theft of hard goods from the warehouse.

Once perceived as necessary only for government and military applications, security is now a growing requirement in the private sector as well. Consider the volumes of customer data and revenue forecasts that could be stolen from a company's sales/marketing database or the evidentiary information gathered by the legal department for a pending lawsuit or patent application. Imagine the impact on individual futures and careers should educational records be compromised or the financial impact of a competitor intercepting engineering designs and confidential product launch strategies.

The government has enacted several pieces of legislation – such as Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, and the Patriot Act – which are intended to protect certain sensitive information. These regulations require organizations to constantly examine their networks and information workflows to make certain that they remain in compliance for records retention/destruction and threats against fraud. In addition, the organization must maintain the privacy of personal, financial, medical, and insurance data.

Canon Goals for Information Security

To better understand the security features offered on Canon's imageRUNNER® Series devices, it is first useful to review the goals of information security: to keep data confidential, to maintain data integrity, and to make data available to legitimate users. Any product that hopes to provide security must achieve these three goals.

Confidentiality

Corporate data may contain information about the organization that should be kept confidential. The goal of confidentiality is to prevent the unauthorized disclosure of information.

Integrity

In addition to keeping data confidential, it must be kept accurate. Integrity assures that data is not altered, either accidentally or with malicious intent.

Availability

Confidentiality and integrity must be achieved while still making data accessible to legitimate users. Controls should be in place to prevent attackers from denying legitimate users access to data and resources.

Government Legislation

The following table briefly summarizes common information security items applicable to MFP devices, as required by current government regulations:

	Requirements	Threats	Potential Mitigation
Sarbanes-Oxley (SOX)	• Section 302 requires executives to certify the accuracy of corporate financial reports. • Section 404 requires executives and auditors to confirm the effectiveness of internal controls for financial reporting. • Section 409 requires any material changes in the financial state of the issuer to be communicated quickly and with supporting data to the public.	Unauthorized access to, or modification of, data; data fraud; data deletion; data availability	User authentication; access controls; encryption (storage and transmission); logging and auditing
Gramm-Leach-Bliley (GLBA)	GLBA has new privacy laws that regulate actions regarding confidential personal information that is collected. For example, data should be encrypted when in storage, data in paper form needs to be secured and disposed of properly and data should only be accessed on a need-to-know basis.	Unauthorized access to, or modification of, data; data fraud; data deletion	User authentication; access controls; encryption (storage and transmission); logging and auditing
Health Insurance Portability & Accountability Act (HIPAA)	Section 164. 312, Technical Safeguards, requires technical policies and procedures for access control on systems that maintain electronic protected health information (EPHI) to be implemented. Also, integrity controls and encryption should be implemented for data in transmission. Audit controls and person/entity authentication mechanisms should be established.	Unauthorized access to, or modification of, data; data fraud; data deletion; audit control	User authentication; access controls; encryption (storage and transmission); logging and auditing
California Information Practice Act CA SB 1386	Organizations must ensure that data privacy is protected and disclose any computer security breaches.	Unauthorized access to, or modification of, data; data fraud; data deletion; audit control	User authentication; access controls; encryption (storage and transmission); logging and auditing
Federal Information Security Management Act (FISMA)	• Sec. 3544 (a)(1)(A)(i) & Sec. 3547: The application should be protected against unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. • Sec. 3544. (a)(1)(A)(ii): Same requirements as the last section, but applies to a contractor of an agency or other organization on behalf of the agency. • Sec. 3544 (b): The application must be able to ensure the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets.	Unauthorized access to, or modification of, data; data fraud; data deletion; data availability	User authentication; access controls; encryption (storage and transmission); logging and auditing

Identifying Key Categories for Device, Network and Document Security

From the summarized table on the previous page, it is obvious that the mitigation mechanisms are all similar in implementation. More specifically, they are as follows:

User Authentication

Every user should establish his or her identity before accessing any resource. Authentication is the method used to verify that the user is who he or she claims to be. The most common authentication mechanisms include passwords, smartcards, and two-factor authentication, such as a combination of a password and card access.

Access Control

Every user's identity is associated with a role and privileges. These decide what the user can access and what actions the user can perform on a given resource. Access controls help protect resources from unauthorized access, modification, and deletion. Role-based access controls (RBAC) are the most common implementation of access controls.

Encryption

The confidentiality and integrity of data must be protected while it is in storage and during network transmission. Protection of data during transmission is commonly achieved through the use of encryption, including Secure Socket Layer (SSL), IPSEC, and algorithms such as TDEA (3DES), AES and RSA.

Logging/Auditing

Audit trails help system owners and auditors confirm that the implemented security mechanisms, such as authentication and access controls, network systems, and application logs are implemented to serve this purpose.

Canon Security Solutions

To help you meet your corporate security goals, Canon imageRUNNER devices may be equipped with a number of defensive solutions that support requirements for data confidentiality, integrity, and availability. From secure printing and document storage to sophisticated identity and device access management, you can trust Canon to deliver solutions that authenticate, encrypt, and preserve data and user histories. Canon's leading-edge security strategy improves your organization's ability to prevent information theft and fraud, while ensuring availability for authorized users.

System Architecture

Before a system is even deployed on a network, it should be properly secured to ensure that it will not introduce new vulnerabilities into the environment or become an easy target. The system should be easy to maintain as new threats emerge and the network evolves. The imageRUNNER device security functionality is implemented early in the design phase and built as an integral part of the system.

Hard Disk Drive (HDD) Protection

Once data has been committed to any nonvolatile storage source there is the potential that it could be compromised. To overcome this reality, imageRUNNER devices utilize a number of proprietary schemes to make the malicious recovery of data difficult to achieve. To further protect the privacy of information, imageRUNNER devices can be further secured through options that utilize either the Advanced Encryption Standard (AES) or Triple Data Encryption Algorithm (TDEA), and powerful overwriting routines. In addition, imageRUNNER devices support Secure Socket Layer (SSL) to ensure the transmission of information is protected over the network.

Device Access Control

Authentication

On the network, the first step of protecting confidentiality and integrity is to ensure that users are who they say they are before they are allowed to access any data or resources. This is accomplished through the process of authentication.

The imageRUNNER device provides various authentication mechanisms, including Department ID Management, Simple Device Log-in (SDL), and Single Sign-On (SSO) authentication. Canon's MEAP development platform also allows for the creation of additional customized authentication applications. For example, end-users can utilize their company's smart card as a way to authenticate at the device.

Access Control

Once a user's identity is confirmed, that identity can be checked against access controls to determine the user's role and privileges as the next step in protecting information. The role and privileges decide what the user can access and what actions can be performed on a given resource. These access controls protect resources from unauthorized access, modification, and deletion. The imageRUNNER device includes various access controls, such as those available through Canon's Access Management System.

Network Access Control

Along with user-access privileges, Canon imageRUNNER devices offer the capability to limit network access to specific IP/MAC addresses and service ports. Network communications can also be further strengthened through support for SSL and IPv6 protocol.

Document Security

To mitigate the risk of confidential information being compromised, documents can be secured through encryption, password-protection, secure watermarks and digital signatures. In addition, using the Encrypted Secured Print feature, documents printed from a desktop computer can be encrypted before sending over the network and held at the device for printing after the correct password has been entered.

In addition, a number of security measures have been implemented within imageRUNNER devices to help protect the information stored in the imageRUNNER Address Book and provide control over the list of authorized recipients.

Fax Security

Features designed to secure the fax functionality such as the separation of fax and network functions through a firewall, fax forwarding, and memory lock are also available on every imageRUNNER device.

Logging/Auditing

For comprehensive auditing of information, Canon offers imageWARE Secure Audit Manager software. This optional software supports Canon imageRUNNER MFPs and LBP printers, and is capable of copying images, text, and attributes of all copy, printer, fax, and scan jobs performed by these devices. Using imageWARE Secure Audit Manager, users can provide extensive audit trails for all document processing activities, creating a deterrent against malicious activity.

These defense solutions are summarized in the table on the following page and are described in detail throughout the remainder of this document.

Summary of Canon Security Solutions and Protection to Help Meet Regulatory Compliance

Protection	Canon Security Solution
System Architecture	• Security-Hardened imageCHIP System Architecture • Proprietary Operating System • Multifunctional Embedded Application Platform (MEAP®) • All MEAP Applications require code signature for installation
HDD & RAM Data Protection	• Data directory information is stored separately • Temporary and permanent data is compressed in a Canon proprietary format and written to random, non-contiguous locations on the hard disk drive • HDD optional security features: - Data Encryption (256-bit AES or 168-bit TDGA (3DES)) - Data Erase (Overwrite up to 3 times) • Standard Job Log Conceal • Hard Disk Drive Format • Mail Box Backup Capability
Authentication & Access Control	• Department ID • Control Card/Card Reader System • Simple Device Log-In (SDL) • Single Sign-On (SSO) • Smart Card Authentication Powered by Codehost (locks entire device) • Access Management System (AMS) (can restrict specific device features) • System Administrator Control • Password Protection for Mail Boxes
Network Access Control	• IP Address Filtering • MAC Address Filtering • Application/Port Access Control • USB Block • Secure Socket Layer (SSL) Encryption • Device Information Delivery Function (DIDF)
Document Security	• Encrypted PDF • Encrypted Secured Print/Secured Print • Watermark/Secure Watermark • Digital Device Signature PDF/Digital User Signature PDF • Address Book Protection - Address Book Password - Address Book Destination Restriction - Access Number Management
Fax Security	• Separation of Fax and Network Functions (Firewall) • Fax Destination Confirmation • Fax Forwarding • Memory Lock
Logging/Auditing	• imageWARE Secure Audit Manager

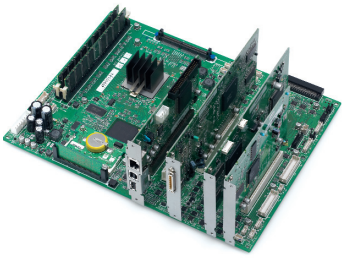
System Architecture

You Take Your Security Needs Seriously. Canon Does Too.

imageCHIP Architecture and Operating System

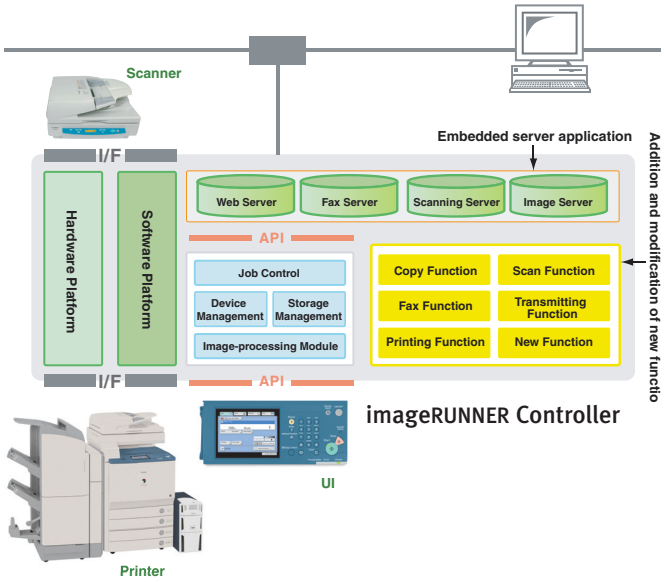
A corporate network will never be secure if the individual systems on the network are not protected against attack before they are deployed, and more importantly, maintained at that same level of security throughout their lifecycles.

Security starts here, with Canon's performance-driven common controller imageCHIP system architecture. Canon's imageCHIP controller technology is the brains inside every imagePLATFORM equipped imageRUNNER device. Its standardized foundation speeds the development and deployment of product enhancements and new functionalities across the entire product line, helping to reduce costs while increasing productivity.



imageCHIP Architecture is at the Heart of Every imagePLATFORM Equipped imageRUNNER Device

Canon's imageCHIP system architecture uses a proprietary, real-time operating system with source code expressly designed by Canon to run embedded applications for imageRUNNER device control. While powerful and adaptable by Canon, it is essentially a closed and proprietary operating system that has been specifically hardened for security purposes and, as such, offers greater protection against those with malicious intents.



Multifunctional Embedded Application Platform (MEAP®)

Canon's MEAP architecture, which is based on the JAVA development platform, provides an environment for customized applications to be embedded within imageRUNNER devices. The MEAP architecture allows the installation of robust applications that are verified by Canon, and are tailored to the needs of particular industries or provide additional capabilities, such as user authentication, device security and integration with other business applications.

MEAP Application: eCopy ShareScan OP

To enhance the security associated with the MEAP development environment, Canon controls access to the MEAP development platform and SDK, making the platform only available to approved developers. Furthermore, application integrity is assured by Canon, as all applications are encrypted and embedded with a digital signature and license. If the application is modified, the attached signature code will not match the original application and, as a result, will not run. In addition, a special key is required that prevents the application code from being accessed. Therefore, it is challenging for anyone to alter a MEAP application or write a rogue application for an imageRUNNER device.

HDD and RAM Data Protection

Canon imageRUNNER devices use a combination of Random Access Memory (RAM) and an internal Hard Disk Drive (HDD) to meet the need for short-term and long-term data processing and storage.

RAM is used for short-term storage of image data during the printing, copying and scanning process. The volatile data stored in RAM is erased and becomes permanently inaccessible once the device is powered down.

The HDD is used to store both short and long-term data such as system control data, user custom settings, system software, application software, driver software, and user image files. For short-term use the HDD stores image data for copy, print, fax and scan functions, which are erased after the transaction has been completed. Image data may also be permanently stored on the hard drive through the imageRUNNER device's Mail Box function. When image data is permanently stored on the hard disk drive, this data is retained even when the imageRUNNER device is powered off.

Hard Drive Data Protection

The imageRUNNER device has the ability to process image data for printing, scanning, faxing, and copying, which creates efficiency in your workflows. It is important to understand how data stored on the imageRUNNER device is securely protected.

Most multifunction products store image data on internal hard disk drives, similar to those found on a personal computer. That data may include scanned images, incoming faxes, spooled print jobs stored temporarily, or files saved in local Mail Boxes for long-term archival and future print-on-demand needs. In addition, similar to that on a PC, the file data remains accessible until that disk sector is overwritten. To safeguard against these common vulnerabilities of hard drive-based storage, Canon has integrated standard security features with its hard disk drive storage capability, thereby significantly reducing the potential threat of data misuse. The ability for thieves to recover usable information from an imageRUNNER device hard drive is made extremely difficult based upon Canon's standard security features, and it is even more challenging when Canon's optional Security Kit is installed and configured properly.

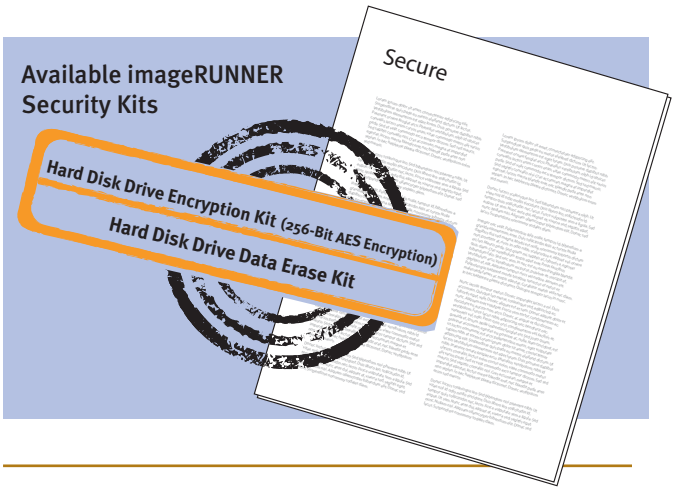
All data, both temporary and permanent, sent to an imageRUNNER device is written in random, non-contiguous locations on the hard disk drive. Data stored on the hard disk drive of imageRUNNER devices is compressed using proprietary formats integral to the operating system, and may only be decoded on the device for increased security. The hard disk drive data directory information for imageRUNNER devices is stored on a separate system board, making file reconstruction infeasible in the event of hard disk drive removal.

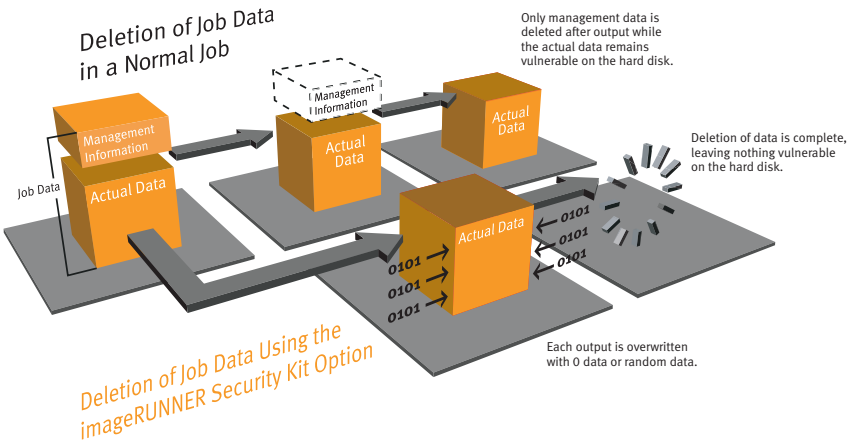
imageRUNNER HDD Security Options

Canon offers optional HDD Security features to further enhance the protection of hard disk drive content. The center of Canon's data protection initiative are Canon Security Kit software and hardware offerings that contain utilities to either encrypt all user data prior to storage on the hard disk and/or initiate the overwriting of the hard disk to completely erase previously stored data. When activated, the Security Kit delivers peace of mind for those in charge of managing sensitive information and serves to meet internal company policies of data protection.

The Security Kit options include:

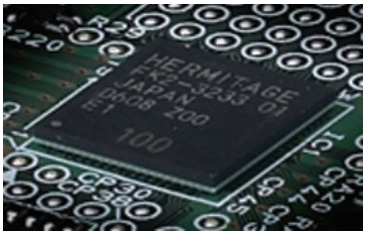
- Hard Disk Drive Data Encryption Kit (256-Bit AES Encryption)
- Hard Disk Drive Data Erase Kit
- Security Kit (Data Erase and 168-Bit TDEA Encryption)





Hard Disk Drive Data Encryption Feature (256-Bit AES Encryption)

Encryption on the hard drive is achieved by using a multi-step process to mitigate any risk of unauthorized disclosure. First, the imageRUNNER device uses mathematical algorithms to scramble bits of data. The data is then encrypted using 256-Bit AES encryption, making the intelligible reconstruction of files infeasible in the event the disk is removed. A secret key is created in the imageRUNNER device, which is stored in a separate system board. This secret key is used to encrypt all image data before writing to the HDD, providing protection for both temporary and permanent data such as documents stored in Mail Boxes. Finally, the data is stored in non-contiguous locations on the imageRUNNER device's hard drive.



MFP Security Chip 1.00 is at the Heart of Every HDD Data Encryption Kit

Hard Disk Drive Data Erase Feature

On most systems that contain a hard drive, once a file is deleted or removed from Hard Disk memory, it is still accessible until it is overwritten. An attacker with the right tools may be able to reconstruct files that have been deleted or have passed through a temporary storage area on the system. For an MFP device, the risk is the same.

Each document that is copied, scanned, printed, or faxed creates some amount of data in temporary storage. With Canon's Hard Disk Drive Erase feature, the data created for each copy, print, scan, and fax job is overwritten and erased immediately after the job is completed; therefore, no trace of the information remains on the hard disk. Choose one of three erasure methods depending on the sensitivity of your documents and applications: overwrite once with null data, overwrite once with random data, and overwrite with random data three times for maximum-security protection.

Overwriting prevents information from being retrieved by data, disk, or file recovery utilities. Overwriting is resistant to keystroke recovery attempts executed from standard input devices and from data hacker tools. The overwriting process includes not only the logical storage location of a file, but also includes all addressable locations. The security goal of overwriting is to replace written data with random data.

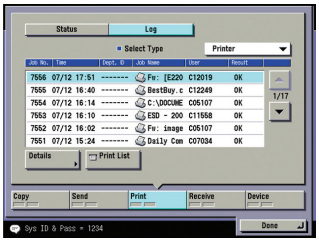
Security Kit

Also available on select imageRUNNER devices is a Hard Disk Drive Data Security Kit which incorporates both Hard Disk Drive 168-Bit Triple Data Encryption Algorithm (TDEA) Encryption and Hard Disk Drive Overwrite functions along with a Job Log Conceal function. The HDD Security Kit is offered as an installable hardware board.

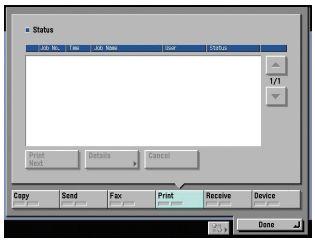
For more information on the availability of security options by device, please refer to the Canon imageRUNNER Hard Disk Drive Security Kit Brochure.

Standard Job Log Conceal Function

The same job history screen that offers traceability can also be concealed from unauthorized users to hide the list of completed jobs, aiding in regulatory compliance.



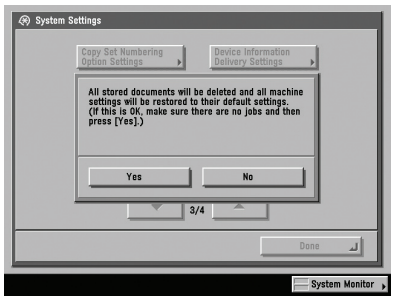
Standard Job Log



Result with Job Log Conceal Enabled

Standard Hard Disk Drive Format

If there comes a time when your imageRUNNER device will be redeployed within your organization or reach the end of its usable life, best practices, and often company policies, usually recommend that systems be completely wiped. The Hard Disk Drive Format feature, which is standard with all imageRUNNER devices, even with no Security Kit installed, completely overwrites all data stored on the hard disk. This includes files, job logs, Address Books, and customized user mode settings, all in a single operation. This ensures that the entire partition containing user data/settings on the imageRUNNER device's hard drive is overwritten and wiped clean before being returned off lease, redeployed elsewhere in the organization, or disposed of, and eliminates concerns of violating your company's security policies.



Use the Hard Disk Drive Format Administration's Screen to Initialize all Data Settings

Mail Box Backup Function

Through Canon's Remote User Interface utility, administrators can manually or automatically backup all documents stored in Mail Boxes and the Job Hold queue to a network file storage destination. For additional security, the backup data is encrypted prior to being sent over the network and can only be restored on the original or upgraded imageRUNNER device.

Common Criteria Certification

The innovative security chip at the heart of Canon's optional HDD Data Encryption Kit and the Security Kit B Series for imageRUNNER devices have received a Common Criteria Certification of Evaluation Assurance Level 3 (EAL3).

Common Criteria

A product awarded Common Criteria Certification (CCC) means it has passed a rigorous government-sponsored inspection process for the safety and security of data entered, stored, displayed, or transmitted by networked devices. Also known as ISO 15408, Common Criteria Certification is a requirement for all hardware and software devices used by government agencies handling national security data. Although not mandatory in the private sector, systems that achieve CCC standards engender a higher level of confidence among IT professionals.

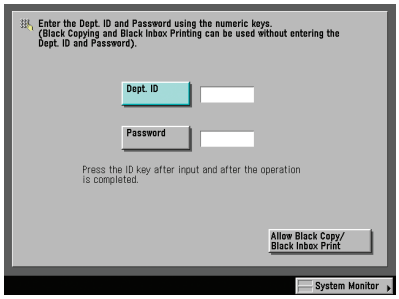
User Authentication

Authentication is the First Step Toward Regulatory Compliance

The proper identification and authentication of every user attempting to access a networked device is critical toward implementing a viable security system. Firms must have controls to restrict physical and virtual access to sensitive information. Depending on the size of your organization and the nature of your documents, Canon offers a number of user identity and tracking tools, ranging from basic to complex, ensuring that only authorized individuals can access system functions, features and data stored on your imageRUNNER device.

Department ID Management

On the more basic end of the scale, Department ID Management allows administrators to configure the imageRUNNER device with valid IDs and passwords for users. This embedded capability restricts system access and/or limits volumes to users, based on their assigned seven-digit ID and seven-digit password. Most imageRUNNER devices support up to 1,000 accounts and track usage by individual, department, or job. This gives administrators the ability to identify users, track job histories, limit volumes, and restrict access to system functions by individual. By registering a Department ID and password for each user, access to the device is limited to those who enter the correct Department ID and password.



Department ID Management Screen

Control Card/Card Reader System Option

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. The Card Reader performs Department ID Management automatically. The optional Control Card/Card Reader system manages populations of up to 300 departments or users.

Simple Device Log-In (SDL) Authentication

SDL is an enhanced version of Department ID Management that grants system access only after verifying an additional personal ID and password. When a user logs on to an imageRUNNER device via SDL, his/her email address is automatically entered into the “From” field of any message sent from the machine. This provides not only authentication, but also non-repudiation. If data is sent from the imageRUNNER device, it can be traced back to the sender with a high degree of confidence.

Single Sign-On (SSO) Authentication

SSO is both easy to administer and use for those in environments utilizing Active Directory. Enterprises with multiple MFPs and/or locations can use SSO to allow employees to access any imageRUNNER device on the network using the same ID and password as they use for their PCs and other networked data-sharing privileges. By utilizing SSO with the optional imageWARE Accounting Manager software, the system administrator can track which users are logging onto each specific imageRUNNER device and the functions they are performing.

imageRUNNER Smart Card Authentication Powered by Codehost

The imageRUNNER Smart Card Authentication for MEAP application provides strong device and data access security for environments that utilize a Smart Card infrastructure. Supporting the most popular Smart Cards and Readers in use today, enterprises can leverage their existing hardware investment to complete the security loop with minimal expense and time. The imageRUNNER Smart Card Authentication Powered by Codehost application quickly and easily performs user authentication at the device with the LDAP/Active Directory server before access is granted and logs their activity for later retrieval if needed. The application can also be configured for PIN-code validation from the control panel for enhanced security. Only upon successful verification with this two-factor authentication can users operate all the functions and features of the MEAP enabled imageRUNNER device.

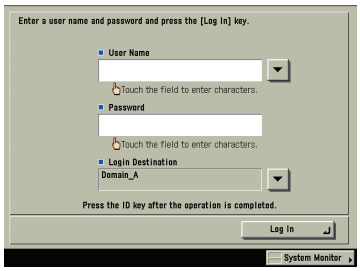
Access Management System

Canon offers two robust tools to limit access to each of the functions and features on imageRUNNER devices at the user and group-level, such as Copy, Send, Fax, Print, Mail Box and Scan. Within each device function, access to individual features or tabs can also be further restricted as a part of the Access Management System. When Single Sign-On has been enabled on a device, users will need to be successfully authenticated at the local device or domain-level before they are permitted access to the functions and features that their role allows.

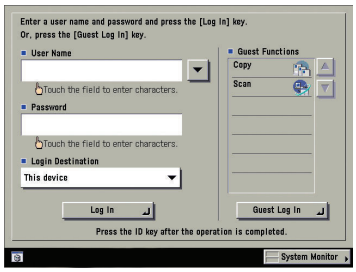
Access to the following functions and features can be restricted:

- Print*
- Copy
- Send (including the Fax function)
- Mail Box (including Job Hold function)
- Web Utilities
- Utilities
- MEAP Applications

Administrators can use the entry-level Access Management System option to define and assign roles on individual imageRUNNER devices. At the enterprise-level**, the imageWARE Access Management System Plug-in for Canon's imageWARE Enterprise Management Console device management software provides centralized administration of multiple imageRUNNER devices.



Single Sign-On Log-In Screen



Access Management System Log-In Screen Containing Guest Login Rights

System Administrator Control

The System Administrator maintains complete control over device settings and end-user accessibility through the use of passwords. This can be accomplished at the device or remotely through Canon's Remote User Interface (RUI) utility, which allows device management and configuration from the desktop.

Password Protection for Mail Boxes

Most imageRUNNER devices offer hard disk drives with a portion of capacity reserved for digital document storage in Mail Boxes. With the ability to store thousands of pages and files for archival, print-on-demand, or collaborative projects, Canon imageRUNNER devices serve as local document libraries as well as output devices. Documents created throughout the day can then be printed and collected in a single trip to the device to maintain privacy and efficiency. Documents intended for specific recipients remain under control with password protection. Administrators retain control of storage limitations to guard against access to files stored in unlocked Mail Boxes. Documents are stored on the internal hard disk drive until deleted, though administrators can also limit storage time of documents stored in Mail Boxes.

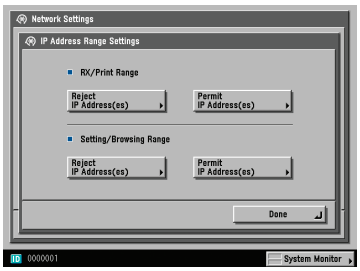
* Printing from a Mail Box can be restricted, but printing from a PC cannot be restricted through the Access Management System.
** Contact your Canon authorized dealer for availability.

Network Access Control

In addition to authentication and user-based access controls, the imageRUNNER device also provides a number of features that deliver protection against network threats. Standard within imageRUNNER devices, administrators can block specific systems and IP/MAC addresses from connecting to the device, as well as access to service ports, applications and connectivity options.

IP Address Filter

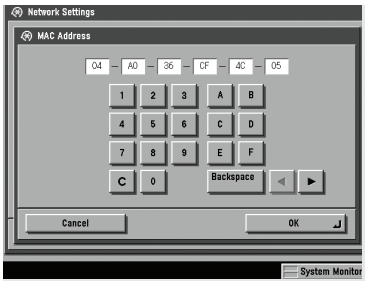
The IP Address Filter on the imageRUNNER device performs a function common to many firewalls. Authorized IT personnel can permit or reject incoming packets from specific IP addresses or range of IP addresses. This allows you to restrict access to the imageRUNNER device for specific users or groups of users based on where they are on the network. Additionally, the imageRUNNER device also allows administrators to apply IP address filters for outbound connections as well. For example, for certain functions such as Remote Copy and Universal Send, administrators can block or restrict end-users from sending files to specific IP addresses. This can help minimize the risk of data falling into the wrong hands by being sent out of the company or to untrusted systems.



IP Address Range Settings Screen

Media Access Control (MAC) Address Filter

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.



MAC Address Settings Screen

Application/Port Access Control

Canon understands that organizations have varied needs and security standards for remote user access and remote administration, and that every open port and enabled service provides another potential path of attack on the system. The imageRUNNER device has been set up to support only the necessary protocols used for transferring data, which are restricted using a network application. Unauthorized access from the outside is blocked through IP-address-based connection and PC-specific MAC address restrictions. Network protocols, such as IPP, FTP, SNTP, SNMP, RAW, LPD, and others, can also be switched on or off at the administrator's discretion. Disabling unneeded services, protocols, and ports assists in securing the network by reducing potential intrusion points.

USB Block

USB Block allows the System Administrator to help protect the imageRUNNER device against unauthorized access. This function may be set to permit or prevent the use of USB Device/Host Interface. System Administrators can use this function when connecting the device to a computer via a USB cable or when connecting a USB device to the imageRUNNER system. When the "Use USB Device" and "Use USB Host" modes are set to "off," USB connections between the imageRUNNER device and a computer as well as the imageRUNNER device and a USB device are prohibited, helping to prevent unauthorized access.

Secure Socket Layer (SSL) Encryption

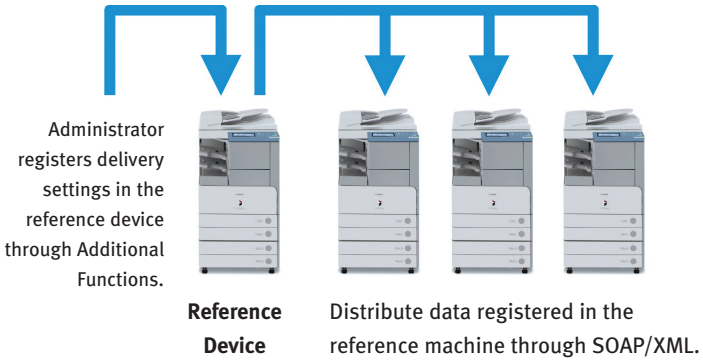
Many organizations are quite diligent about protecting data as it is transferred between PCs and servers or from one PC to another. However, when it comes to transmitting that same data to and from the MFP device, it is almost always sent in clear text. As a result, it may be possible to capture all 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 scan-to-email, Internet-fax (i-fax), Remote UI, Web Access and DIDF.

As a communications hub, imageRUNNER devices are capable of connecting your business with high-speed information distribution capabilities through Canon's Universal Send technology. By leveraging the power of your existing data network infrastructure, you can scan and send TIFF, PDF, and JPEG files to any network destination–email addresses, network servers, file folders, and Internet fax numbers. Even though scanned data is just passing through your MFP, data streams can be intercepted as they travel to their intended destinations. Canon imageRUNNER devices utilize SSL technology to encrypt the content of emails and i-faxes when sending to authorized destinations. SSL for scan and send provides transport layer security to ensure documents scanned on an imageRUNNER device are safely transmitted to the recipient.

Device Information Delivery Function (DIDF)

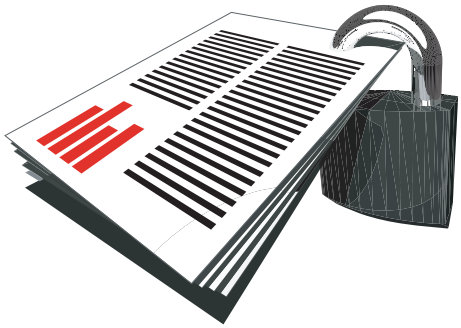
Device Information Delivery Function (DIDF) allows the administrator to easily manage and maintain imageRUNNER devices over a network and ensures that these devices are configured in accordance with the company's security policy. The administrator sets an imageRUNNER device as a reference machine and the management data can be distributed and registered automatically to up to 100 other specified imageRUNNER devices on the network. Data that can be managed includes the Address Book, Forwarding Settings, Favorites Keys, Department ID, and settings entered in [Additional Functions].

Device Information Delivery Function



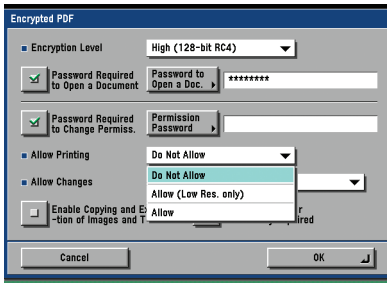
Document Security

Canon imageRUNNER devices are equipped with a host of features and functions to help minimize accidental disclosure of data to casual observers. From basic face-down output to secure printing, Canon protects your information with the following security technologies.

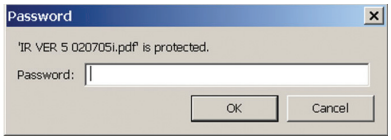


PDF Encryption

In addition to SSL encryption for sending scanned documents, the imageRUNNER device also uses Adobe® standards to allow users to scan and send documents as encrypted PDF files. This is performed directly at an imageRUNNER device equipped with Universal Send, without the need for additional software. PDF Encryption provides an additional layer of security beyond SSL, and helps to ensure that documents are still secured once they reach their destination. By requiring a password to open the document or to print, change, or extract data, PDF Encryption gives businesses increased control over documents, even after they leave your hands. For even greater protection, the password itself can be encrypted to further restrict unauthorized users from viewing documents. Users may select either 40-bit or 128-bit encryption.



PDF Encryption Screen

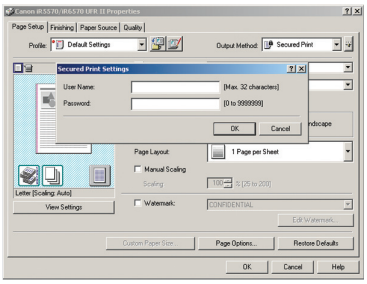


Encrypted PDF Password Prompt

Encrypted Secured Print/Secured Print

Encrypted Secured Print and Secured Print are essentially delayed, authenticated print features that hold a print job in queue on the imageRUNNER until the user enters a specified password authenticated at the device to release the job. This ensures that the user is in close proximity when the document is printed. The imageRUNNER device requires the user to set a password in the print driver window when sending a print job from a connected PC. With Encrypted Secured Print, the data transmitted across the network is encrypted and automatically deleted once printing has been completed.

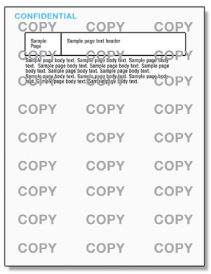
Secured Print Screen on PC Print Driver



Watermark/Secure Watermark

Watermarks allow users to embed owner information in documents, which can be retrieved in either its printed or digital form. Secure Watermarks allow users to embed hidden text that becomes visible when the document is copied, deterring the making of unauthorized copies. Watermarks and Secure Watermarks work by inconspicuously embedding coded information in the document, much like the ones used in bank notes.

Document with Embedded Hidden Text from the Secure Watermark



An Unauthorized Copy of a Document with the Secure Watermark

Digital Device Signature PDF/Digital User Signature PDF

Canon imageRUNNER devices offer the ability to add components that help prevent impersonation and provide information of any alteration. With the Device Signature Feature of the Universal Send PDF Security Feature Set (standard on color "i" models; optional on "base" models), administrators can install a digital certificate that users can add to a PDF file, which embeds the device name, serial number and time/date stamp to provide verification of the source device. The device signature will also provide notification in the event changes are made. 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 Protection

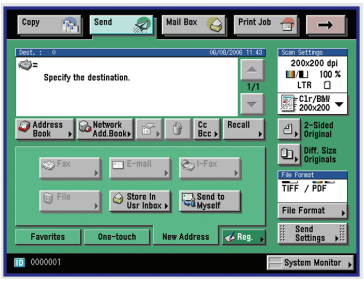
A number of security measures have been implemented within imageRUNNER devices to help protect the information stored in the Address Book and provide control over the destination types that can be used.

Address Book Password

Administrators can enable the password-protection feature on the imageRUNNER device to control access to the data stored in the Address Book. Once enabled, users must enter the correct password on the device to add, change or delete entries. This helps ensure that only authorized recipients receive documents.

Address Book Destination Restriction

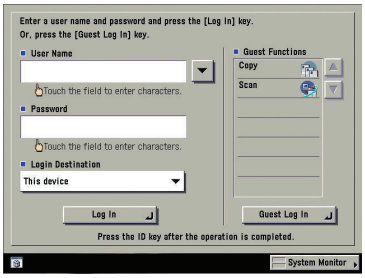
Users can be restricted from adding new addresses by specified destination type such as fax, emails, i-fax and file when sending documents through Color Universal Send. Each restricted destination type will be grayed out and unavailable for selection on the Send interface of the device. When enabled, users may only select addresses registered in the address book.



Color Universal Send Destination Restriction Function Screen

Access Number Management

To shield the Registered address from being viewed by users browsing the address book, administrators can assign an Access Number to hide its visibility unless the proper code has been entered on the device control panel.



Access Number Management Screen

Fax Security

Canon Fax Boards Have Firewall Protection

Since the advent of MFPs, there has been a misconception about the possibility of network penetration via the public switched telephone network (PSTN) used for voice and fax transmission. Canon imageRUNNER devices may be equipped with a G3 fax board. To help prevent network penetration via the public switched telephone network, the imageCHIP system architecture's firewall physically and logically separates the fax modem from network functions residing on the main controller board. The G3 fax board implementation connected to the public switched telephone network responds only to CCITT.T30 commands and does not support network communication protocols, preventing hackers from initiating a malicious network attack via the fax port on a Canon imageRUNNER device. Only G3 Fax protocol data can be exchanged; otherwise, the circuit is disconnected with a fax error code.

The imageRUNNER device's Fax Board does not come with a binary transfer function and, therefore, it is not possible to receive data files other than fax image files. In the very unlikely event that the fax board did receive a data file that "pretended" to be a fax image data file, the call would be disconnected and result in a fax error code.

Fax Destination Confirmation

To help prevent faxed documents from being inadvertently sent to the wrong destination, imageRUNNER devices 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 Forwarding

This function allows select imageRUNNER devices equipped with a fax board to forward inbound fax transmissions to specific recipients or destinations. 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.

Memory Lock

Documents received by select imageRUNNER devices equipped with a fax board may store incoming fax documents into a memory reception box until the recipient is available to print and accept them. This user-selectable feature allows a department or company to maintain document hardcopy security over their received documents until they are ready to physically retrieve them. This is good for high-traffic areas where users cannot immediately pickup incoming faxes.

Logging/Auditing

imageWARE Secure Audit Manager

To help protect confidential data, reduce the impact of information loss and assist in meeting strict government guidelines, Canon's proprietary imageWARE Secure Audit Manager software provides tracking and accountability of documents sent to and from Canon imageRUNNER and imageRUNNER LBP devices. Ideal for government, legal, finance and educational organizations, imageWARE Secure Audit Manager is the first product that provides hardcopy document distribution transparency for all print, scan, fax, copy and send jobs. In an effort to deter information leakage, crucial data such as the user ID, time/date, send/receive and an indexed record of what was sent can easily be searched and retrieved.

imageWARE Secure Audit Manager captures all job log information, along with it's image and text data, and stores it in a central repository to create a complete and detailed audit trail. Once captured, information can be retrieved using one of three search features: image search provides the ability to locate documents based upon images contained within the document itself, full-text search finds matches from patterns of words, and attribute search enables the identification of matches based on device name, job log ID, IP address and more. To aid in proactive leak detection, administrators can enable Keyword Notifications to send alerts via email when designated phrases are detected in copy, fax, scan, print, and send jobs.

Conclusion

Awareness is the key to initiating your security process, while regulations are a means to enforce implementation of proper controls regarding data security. Security threats have emerged to target networked MFPs in the office. Your organization needs to implement a security solution that will protect your data from fraud, unauthorized access, modification, and deletion. Canon understands your security requirements and has developed security capabilities that help mitigate the risk to your data.

Even the most well conceived security plan is subject to some penetration threat through the variables of workflow, document distribution capability, and employee motivations. However, by utilizing the security features of a Canon imageRUNNER device, you can help in effectively aligning security with corporate goals, protecting company assets, and achieving compliance with federal regulations.

From the imageCHIP system architecture to digital watermarking, Canon improves data security whether you are printing, scanning, emailing, faxing, or copying. Ask your Canon Representative for more information about how imageRUNNER security solutions can help achieve the confidentiality, data integrity, and availability of information across your organization.

Canon
imageANYWARE

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

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