Security Features

How Secure Is Your MFP?

Companies today spend an incredible amount of their time, money, and resources in securing their information systems. Regulations, such as the Gramm-Leach-Bliley (G-L-B) Act and HIPAA, actually mandate that firms protect their confidential information.* As a result, IT administrators and business managers are forced to constantly examine their networks and business processes to ensure they are in compliance. And ever since MFPs have become a mainstay in network environments, Canon imageRUNNER® devices are subject to intense scrutiny to ensure that they are not vulnerable. Fortunately, Canon has equipped the imageRUNNER with many security features that can put the security-conscious decision-maker at ease.

Solution

Security Features of the Canon imageRUNNER

When looking at a security landscape, experts and IT administrators generally identify and focus on five key areas:

1. **Passwords and Authentication**
2. **Compression and Encryption**
3. **Data Control**
4. **Data Erase**
5. **Network Security**

With the complex nature of the Canon imageRUNNER device, its imagePlatform architecture, and its many capabilities, several security features overlap into multiple categories. However, most will fit well into one main category to satisfy IT and corporate security demands.

How Do You Do It?

1. Passwords and Authentication

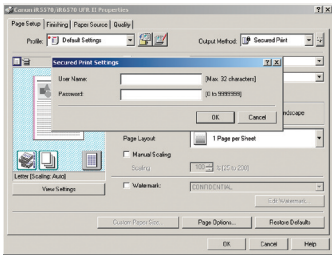
System Manager Security

- Many high-function features of the imageRUNNER device can be protected from modification without authentication.
- This prevents unauthorized changes to the security and functions of the device, and helps maintain the security environment created by the IT administrator.

Mail Box Print

- Users may print to an imageRUNNER Mail Box as opposed to an unattended output tray. Documents are stored on the internal hard disk until deleted.
- Mail Boxes may be password-protected for security.
- To enforce document security policies and protect information in nonpassword-enabled Mail Boxes, administrators can limit storage time of Mail Box documents via System Manager.

Secured Print



- This function helps limit accidental disclosures of sensitive information when printing to a publicly accessible imageRUNNER device by allowing users to assign each document a unique password.
- The job is held in the imageRUNNER device's RAM until the user releases the job by entering a password on the control panel.
- Secured Print jobs are not stored to the hard disk and are deleted from memory upon job completion.

User Authentication

- To maintain control over IT environments, administrators can restrict printing, copying, faxing, or e-mailing documents to authenticated users. The restrictions aid in maintaining a tight information security environment.
- In order of increasing security, the three authentication levels are as follows: Department ID Mode, SDL (Simple Device Log-In), and SSO (Single Sign-On). SDL and SSO are more secure, as they work with network-based authentication servers to grant access.

2. Compression and Encryption

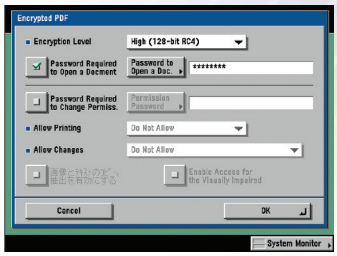
Native Compression

- All data stored on the hard disk is compressed using the JBIG file format.
- Compressed data can be read only by an imageRUNNER device using a Canon proprietary JBIG format integral to the operating system, thus making stored data highly secure.

Hard Disk Security

- The optional imageRUNNER Security Kit-A2 encrypts all data stored on the hard disk using 168-bit encryption, preventing access in the event the hard disk is removed.
- The imageRUNNER Security Kit-A2 also conceals the list of completed jobs to unauthorized users.

Encrypted Send



- An upgrade to Universal Send™, PDF Encryption allows users to scan documents and send an encrypted PDF file right from the imageRUNNER device, without the need for additional software.
- PDF Encryption gives users and businesses control over sent documents by requiring a password to open the document or to print, change, or extract data.
- PDF Encryption uses security features that are consistent with Adobe® standards, including 128-bit encryption.

3. Data Control

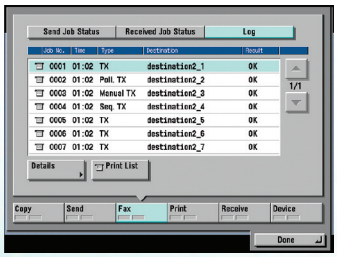
Hard Disk Security

- The Image Platform operating system provides data security to reduce the risk of print/copy/fax jobs and stored documents being retrieved by an unauthorized person.
- The hard disk directory information is stored on a separate system board, not on the hard disk itself.
- The optional Removable HDD** provides businesses with additional security via an option to readily remove the HDD and store it in a secure place.

Secured Print

- This function helps limit accidental disclosures of sensitive information by allowing users to assign a password to a document when printing from a PC.
- The job is held in the imageRUNNER device's RAM until the user releases the job by entering a password on the control panel.

Job Logs



- All imageRUNNER models maintain detailed logs of user activity, including print, copy, and send functions.
- By enabling one of the three authentication modes, activities can be matched to individual users as an aid to activity tracking and regulatory compliance such as HIPAA and Gramm-Leach-Bliley (GLBH), Section 501B.

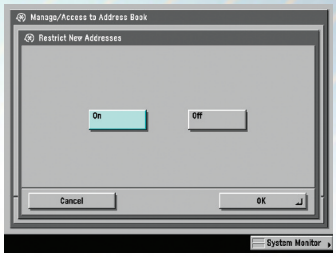
Memory Lock

- Instead of collecting on an open output tray, in-bound fax or I-fax documents can be stored automatically in a separate Memory RX Inbox on the hard disk.
- When turned on, Memory Lock may be active at all times or only when scheduled (for example, unattended hours).
- The Memory RX Inbox may be password-protected so only authorized users may retrieve held documents.
- Users can print, view, or forward documents from the Memory RX Inbox.

Fax Forwarding (for Fax and I-fax Documents)

- Rather than collecting on an output tray, inbound documents can be forwarded to an attended fax device, e-mail address, network location including file server, or Confidential Inbox on the imageRUNNER device.
- Jobs can be forwarded under certain conditions (such as from a particular area code), or unconditionally to aid compliance, tracking, or workflow. Multiple job forwarding conditions can be enabled.

Restrict Access to Destinations



- When users are sending documents from an imageRUNNER with Universal Send, administrators can restrict the send destinations to the preprogrammed Address Book.
- When used in conjunction with an Address Book password, this feature helps protect information by helping ensure that data is sent only to authorized e-mail, fax, or network locations for environments with information security regulations such as SEC, and HIPAA and G-L-B Acts.

Fax Security

- The design of the imageRUNNER network and fax systems ensures that remote access and data activities cannot take place via the fax modem.
- While a received fax document can be accessed through a network connection via the Web-based Remote UI™ function or a forwarded fax communication, it's not possible to breach security, as these functions are available only after completion of the fax communication.
- The Super G3 Fax Board only can decode fax transmissions; therefore, any attempt to send a file to the imageRUNNER device via fax cannot be processed.

Face-Down Output

- imageRUNNER 70 Series models (5570 and higher) can force documents to output face-down, helping to prevent accidental disclosure of data to casual observers in an open office environment.
- Many healthcare entities have adopted a policy of face-down printing as a way to comply with aspects of HIPAA Privacy and Security rules.

4. Data Erase

Hard Disk Security

- Data is written in random, non-contiguous locations on the hard disk drive. The data's directory location is erased immediately after job completion.
- The Initializing All Data/Settings Mode allows the user to erase all data on the hard disk (image data, logs, address books, and user-mode settings) to address concerns about leaks or theft of data when a device is moved, returned through a lease, or otherwise disposed of. (imageRUNNER 70 Series models, other than the 5570/6570, require firmware upgrade.)
- The optional imageRUNNER Security Kit also can encrypt data stored on the internal hard disk and wipe latent data after jobs have been completed using one of three levels of disk wipe.

Secured Print

- Secured Print jobs are held in the imageRUNNER device's RAM until the user releases the job by entering a password on the control panel.
- These jobs are not stored to the hard disk and are deleted from memory upon job completion.

5. Network Security

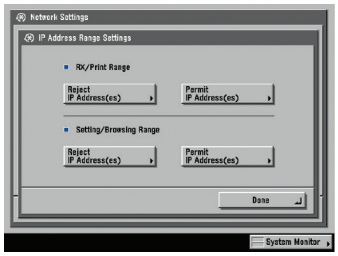
Network-Friendly Architecture

- The imageRUNNER device is a network-friendly resource, offering seamless integration into existing networks and allowing administrators the flexibility required to run efficient, well protected IT environments.
- By offering a high level of self-protection through various configuration and protocol options, the Canon imageRUNNER device helps protect the larger network.

Blocking Services, Protocols, and Ports

- An administrator can control services and protocol as well as port usage by turning individual functions on or off if not in use. Network protocols such as IPP, FTP, SNTP, RAW, LPD, and others can be switched on or off at the administrator's discretion.
- Disabling unneeded services, protocols, and ports assists in securing the device and the network by reducing potential intrusion points.

Setting IP Ranges



- Administrators can set the imageRUNNER device to *permit* or reject a particular IP address or range of addresses when setting up a device on the network.
- Utilizing this function provides permission for network resources to access the device on the network. This function also gives administrators the capability to block/restrict a particular end-user or set of end-users based on IP addresses.

MAC Address Filtering

- MAC Address Filtering allows the administrator to specify which MAC addresses can access the imageRUNNER device. The MAC address is each computer's unique network hardware number. When MAC Address Filtering is enabled, only specified network resources may communicate with the device.

Secure Socket Layer (SSL)

- Secure Socket Layer encrypts data communications between client PC and a server for Remote UI, e-mail/I-fax, IPP printing, and device information distribution functions (uses HTTPS over SSL).

NOTE: Some functions described above require optional equipment.

FAQ

Q: Can I remove data from an imageRUNNER device hard drive when my lease is over?

A: Yes. The Initialize All Data/Settings function erases all data from the hard drive and resets all settings to the factory default. (The imageRUNNER '70 Series models, other than 5570/6570, require firmware upgrade.)

Q: What is the difference between printing to a Mail Box and using Secured Print?

A: When using Mail Box print, the document is stored to a particular Mail Box on the imageRUNNER hard drive. After a user retrieves the document it remains stored on the hard drive (unless additional action is taken). Users who can access the Mail Box can access all documents stored in that box.

Secured Print requires a user to select a unique password when the document is printed from the PC. The document is stored only in the imageRUNNER device's RAM. Releasing the document requires the user to enter the password chosen at the PC. After printing, the document is immediately erased from memory.

Q: Can I restrict users' access to the imageRUNNER device from a computer?

A: Yes. Administrators can set Job Accounting to require that a user enter an administrator-defined password to print a document to an imageRUNNER device. IP address ranges can be set to permit or reject access for printing and Remote UI operations. Also, MAC addresses can be set to specify what unique devices may access an imageRUNNER device. Since IP addresses can change and MAC addresses are more difficult to fake, this is the more secure method.

Q: Can I restrict access to walk-up features of an imageRUNNER device?

A: Yes. Administrators can specify one of three levels of authentication: Department ID, Simple Device Log-On (SDL) or Single Sign-On (SSO). Department ID is the most simple, with all Department IDs and passwords stored locally on the imageRUNNER device. SSO is the most secure, authenticating users against your corporate ActiveX directory server and with their standard network log-on credentials.

Q: Is the imageRUNNER operating system susceptible to viruses?

A: The Image Platform operating system uses a proprietary Canon architecture not used by other systems or companies. As a result, it has not been a focus of activity by the hacker community. The IP operating system has number features to help prevent malicious attacks from damaging either the imageRUNNER device or the network.

Q: Can an unauthorized or malicious program be loaded onto an imageRUNNER device's Java-based MEAP® platform?

A: No. Canon's Multifunctional Embedded Application Platform (MEAP) has numerous safeguards to prevent unauthorized applications from being loaded onto an imageRUNNER device; only applications that have received approval by Canon and have a valid key can be installed.

Q: Can the contents of an imageRUNNER device hard drive be encrypted? Can data be purged after jobs are completed?

A: Yes. The imageRUNNER Security Kit-A2 encrypts the contents of the hard drive with 168-bit encryption. It also can wipe job data from the hard drive after the job is completed or erased from a Mail Box.

Q: Can the contents of a Mail Box automatically be purged after a set time?

A: Yes. Administrators can set Document Auto Erase for each Mail Box. Documents can be set to expire in increments of hours or days, or set for no expiration. The default is three days.

Q: Is there a way to periodically and automatically reset an imageRUNNER device to a certain configuration to help enforce the corporate security policies?

A: Yes. The Device Information Delivery Settings function allows administrators to set one imageRUNNER '70 Series device as a reference and distribute that configuration to other '70 Series models. Administrators can distribute settings for Address Books, Department IDs, System Manager, Copy, Communications, and many others. Device Information Delivery Settings function can automatically broadcast settings from the reference device daily or at a time and schedule set by the administrator; these are transmitted using SSL security.

Canon KNOW HOW®

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

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

* *Does not constitute legal advice. For complete information on compliance with these statutes, you should consult with your legal counsel.*

** *Check with your local Authorized Canon Dealer for availability.*

0405-SEC-PDF-NR

imageANYWARE℠