

Canon Security Features

Due to the vital nature of government information, safeguarding it has never been more important. Canon recognizes this important need and, as a result, has developed comprehensive security capabilities across our entire imageRUNNER product line.

1. Passwords and Authentication

System Manager Security

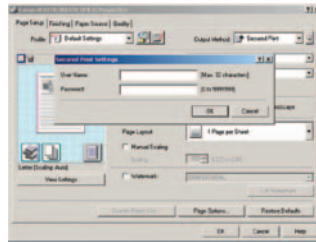
- Many high-function features of the imageRUNNER device can be protected from modification without authentication.
- This prevents unauthorized changes to the security and functions of the device, and helps maintain the security environment created by the IT administrator.

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

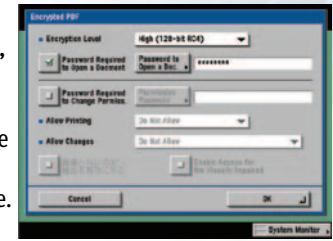
- All data stored on the hard disk is compressed using the JBIG file format.
- Compressed data can be read only by an imageRUNNER device using a Canon proprietary JBIG format integral to the operating system, thus making stored data highly secure.

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

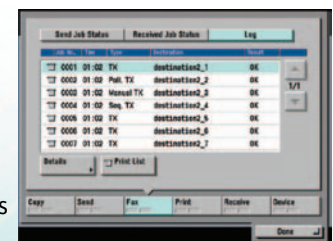
- The Image Platform operating system provides data security to reduce the risk of print/copy/fax jobs and stored documents being retrieved by an unauthorized person.
- The hard disk directory information is stored on a separate system board, not on the hard disk itself.
- The optional Removable HDD** 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

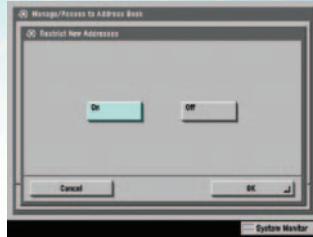
- Instead of collecting on an open output tray, in-bound fax or I-fax documents can be stored automatically in a separate Memory RX Inbox on the hard disk.
- When turned on, Memory Lock may be active at all times or only when scheduled (for example, unattended hours).
- The Memory RX Inbox may be password-protected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

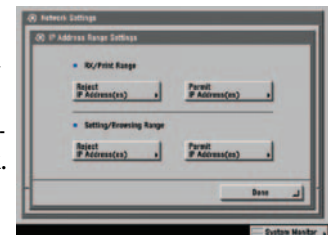
- The imageRUNNER device is a network-friendly resource, offering seamless integration into existing networks and allowing administrators the flexibility required to run efficient, well protected IT environments.
- By offering a high level of self-protection through various configuration and protocol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