



Security Solution Sheet

Canon's imageRUNNER ADVANCE series of multifunction devices offer a wide variety of standard and optional security solutions which can address your concerns regarding the protection of confidential data.

Hard Disk Drive Data Confidentiality

Once a document is copied, scanned, printed or faxed, image data resides on the hard drive of the device. To assist customers who are looking for advanced Hard Disk Drive security during active device usage, features such as *HDD Data Erase*, *HDD Data Encryption*, *HDD Lock*, and *HDD Data Erase Scheduler MEAP* are available. At the time of removal of the device, Canon offers a standard *Hard Disk Drive Format* feature which completely overwrites all data stored on the hard disk with null data at the end of device use. The next generation imageRUNNER ADVANCE Series offers a standard 9x overwrite at time of HDD Format.

Device Security

For environments with the highest security concerns, Canon next generation imageRUNNER ADVANCE systems are IEEE 2600.1 certified. The IEEE 2600.1 is a global information security standard for hard copy devices that require a high level of document security, operational accountability and information assurance. With specified processes, configurations and settings implemented upon installation, Canon's systems are certified to achieve and maintain the necessary requirements as defined in IEEE 2600.1 standard.

MFP Device Access & Control

imageRUNNER ADVANCE systems include a number of authentication options which administrators can use to ensure that only approved users can access the device and its functions, such as print, copy and scan and send features. To facilitate device user authentication, customers can choose to use a standard device based authentication method or an optional card

based method whether embedded or server based. For Federal Government agencies, Canon provides CAC/PIV card authentication for device access, as well as secure document distribution. For MFP function access control, Canon offers solutions that can lock down the entire device, or simply restrict users or groups to only specific functions

Auditing

Standard on Canon imageRUNNER ADVANCE devices is the Job/Audit log which provides administrators the ability to track and audit device usage. Additionally, Canon offers solutions which can provide a more in depth, ongoing audit log for those customers who wish for an even more comprehensive audit log.

Document and Information Security

Canon offers a number of ways to secure documents generated and managed by Canon hardware and software technologies. Canon's solutions include secured & follow me printing, document password protection, encryption, document rights management, and destination restrictions.

Network Security

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. imageRUNNER ADVANCE systems offer IPsec and IPv6 support, which provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4.





Security Features	iR-ADV C9000PRO/ C7000/C5000/ C2000 Series	iR-ADV 8000/6000/ 4000 Series	iR-ADV C5200/C2200, 6200/8200, C7200/C9200 PRO, 500iF/400iF, 4200 Series	iR-ADV C350iF C250iF
Device Based Authentication				
<i>Device Based</i>	s	s	s	s
<i>Active Directory/SSO</i>	s	s	s	s
Card Based Authentication				
<i>Proximity Card or CAC/PIV</i>	o	o	o	o
Access Control				
<i>Password Protected System Setting</i>	s	s	s	s
<i>Access Management System</i>	s	s	s	s
<i>USB Block</i>	s	s	s	s
Data Security				
<i>Hard Drive Data Format(EOL)</i>	s (1x)	s (1x)	s (9x)	s (9x)
<i>Hard Drive Data Encryption</i>	o	o	o	o
<i>Hard Drive Data Erase</i>	o	o	s	s
<i>Removable Hard Drive Kit</i>	o	o	o ⁶	NA
<i>HDD Data Erase Scheduler MEAP</i>	NA	o ⁴	o ⁵	o ⁵
<i>HDD Password Lock</i>	NA	s ¹	s	s
<i>TPM (Trusted Platform Module)</i>	s	s	s	s
Document Security				
<i>Secure Print (Driver Based)</i>	s	s	s	s
<i>Secure Print (Server/Serverless)</i>	o	o	o	o
<i>Mail Box Security</i>	s ²	s	s ²	NA
<i>Encrypted PDF</i>	o	o (AES-256 bit) ³	o (AES-256 bit)	o (AES-256 bit)
<i>Document Scan Lock</i>	o	o	o ⁶	NA
Network Security				
<i>Port Management, IP Address & MAC Filtering</i>	s	s	s	s
<i>IPSEC</i>	o	s ¹	s	s
Certifications				
<i>IEEE 2600.1</i>	Certified C5000 Series ⁷	Certified 4000 Series ⁷	Certified ⁷	Pending ⁷
<i>Common Criteria Certified (EAL3)</i>	HDD Encryption	HDD Encryption	HDD Encryption	HDD Encryption

Footnotes:

- 1 Standard on iR-ADV 4000 Series Only
- 2 Not available in the iR-ADV C2000/C2200 Series or 500iF/400iF Series
- 3 AES-256 bit support only for iR-ADV 4000 Series
- 4 imageRUNNER ADVANCE 4000 series with firmware V 19.02 or higher
- 5 imageRUNNER ADVANCE 5200 series with firmware V 17.10 or higher
- 6 Not available in the iR-ADV 500iF/400iF Series
- 7 Check Canon USA Website for latest list of Certified Models

Table Key:

s= Standard to device o=Optional to device

Please refer to your Service Provider, and also the Canon USA website at usa.canon.com for most complete and up-to-date information

Canon and imageRUNNER are registered trademarks of Canon Inc. in the United States and may also be registered in other countries. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Specifications and availability subject to change without notice.



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

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

