

SECURITY PROFILE SHEET



Canon's imageRUNNER ADVANCE Series of multifunction devices offers a wide variety of standard and optional security features, which can help users protect documents and limit access to data.

Device Security Features*

Canon imageRUNNER ADVANCE systems include a number of authentication options to help ensure that only approved users access the device and its functions. To facilitate device user authentication, customers can use a standard, device-based authentication method or an optional, card-based method (embedded or server-based). For federal government agencies, Canon provides optional CAC/PIV card authentication for device access and document distribution.

Universal Login Manager is a server-less solution for imageRUNNER ADVANCE devices, offering simple log-in and usage tracking functionalities. It delivers convenient user authentication and allows organizations a way to manage access and costs by controlling individual users' access and usage.

When a document is copied, scanned, printed, or faxed, image data resides on the hard drive of the device. For advanced Hard Disk Drive (HDD) security during active device usage, available features include *HDD Data Erase*, *HDD Data Encryption*, *HDD Lock*, and *HDD Data Erase Scheduler MEAP*. At the time the device is removed or at end of life (EOL), Canon offers a standard *HDD Format (9x overwrite)* feature that overwrites data stored on the hard disk with null data. There's also a *Removable HD Kit* that allows for physical removal of the hard disk.

Document Security Features*

Canon offers several ways to help limit access to documents generated and managed by Canon hardware and software technologies. Canon offers solutions including Secure Print secured and Follow-me printing, document password protection,

encryption features, document rights management, and destination restrictions.

Network Security Features*

Standard network security features include the ability to set up the device to permit only authorized users and groups to access and print to the device. This helps limit device communications to designated IP/MAC addresses and controls the availability of individual network protocols and ports.

Canon imageRUNNER ADVANCE systems offer IPsec is a protocol for facilitating the security of IP packets sent and received over an IP network by helping to protect from threats such as theft, modification, and impersonation.



* Depending on the model, some features are within the standard feature-set of the device, while others require additional accessories. Please see page two of this document or contact your local Canon Authorized Dealer for more information.



Product Family	Third Generation imageRUNNER ADVANCE	Third Generation imageRUNNER ADVANCE Second Edition
Security Features	C7500 Series, C5500 Series, C3500 Series, C355iF/C255iF, 8500 Series, 6500 Series, 4500 Series	C7500 II Series, C5500 II Series, C3500 II Series, C356iF II Series, 8500 II Series, 6500 II Series, 4500 II Series
Security Management		
Security Policy Settings	Standard	Standard
Device-Based Authentication		
Device-Based	Standard	Standard
Active Directory/SSO	Standard	Standard
Universal Login Manager	Standard	Standard
Card-Based Authentication		
Proximity Card or CAC/PIV	Optional	Optional
Access Control		
Password-Protected System Setting	Standard	Standard
Access Management System	Standard	Standard
USB Block	Standard	Standard
Data Security		
TPM (Trusted Platform Module)	Standard	Standard
Hard Drive Password Lock	Standard	Standard
Hard Drive Data Format (EOL)	Standard (9x)	Standard (9x)
Hard Drive Data Erase	Standard	Standard
Hard Drive Data Erase Scheduler MEAP	Optional	Optional
Hard Drive Data Encryption	Standard (FIPS 140-2 Validated)	Standard (FIPS 140-2 Validated)
Hard Copy and System Security	Optional (IEEE 2600 Common Criteria)*	Optional (IEEE 2600 Common Criteria)*
Removable Hard Drive Kit	Optional/NA**	Optional/NA**
Document Security		
Secure Print (Driver-Based)	Standard	Standard
Encrypted Secure Print (Driver Based)	Optional	Standard
Secure Print (Server/Serverless)	Optional	Optional
Secure Watermark	Optional	Standard
Mail Box Security	Standard	Standard
Encrypted PDF (AES 256 Support)	Optional	Standard
Device Digital Signature PDF	Optional	Standard
Document Scan Lock	Optional	Optional
Network Security		
Port Management, IP Address, MAC Filtering	Standard	Standard
IPsec	Standard	Standard
Cipher Algorithm Selection	Standard	Standard
TLS1.1/1.2 Supported and SSL 3.0 Disable	Standard	Standard
Certifications		
Common Criteria IEEE 2600*	Optional*	Optional*
FIPS 140-2	IPSEC/CAC/PIV/HDD Encryption/TLS	IPSEC/CAC/PIV/HDD Encryption/TLS

* IEEE 2600 Kits may not be available at the same time of product release; check with your Canon Authorized Dealer for availability.

** Not available with the imageRUNNER ADVANCE C365iF/C255iF and C356iF II/C256iF II Series.

Canon