Canon

imageRUNNER ADVANCE Solutions

SECURITY

Safeguarding Information Within Documents and Devices

ADVANCE to Canon MFP security solutions.

Whether your business relies on paper documents, electronic documents, or both, you need to ensure that any sensitive information within them can only be accessed, retrieved, or distributed by authorized users.

Canon imageRUNNER ADVANCE device and software solutions help you support your security policy goals by protecting any file that is sent, stored, or printed.

Control device access and restrict usage by user, group, function, and more.

Generate documents that maintain security even after printing and distribution.

Be confident data on system is secure and protected.

Safeguard document information from network breaches.

imageRUNNER ADVANCE

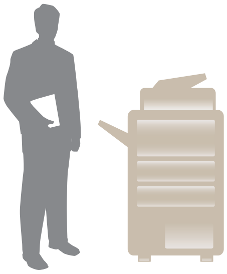
Need to control who has access to your MFPs and MFP functions?

Businesses may benefit from each new technology advance. But decision makers must ensure that all devices and software added to a network include control and access features to help prevent theft, misuse, or information leaks.

Are there easy ways to secure our MFP devices?

How can we maintain high levels of security without impeding productivity?

Is it possible to control MFP feature access on a per-user basis, depending on their authentication levels?



Can employees use their current building access IDs and PC login passwords at the MFP?

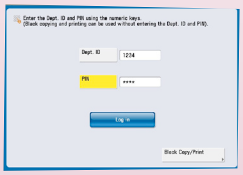
Are there ways to prevent staff from sending documents out to unauthorized recipients?

Device-Based Authentication

Controlling the device begins with authentication by the user. Canon offers a wide range of ways to authenticate at your imageRUNNER ADVANCE system, and many work well with existing directory systems you may already use.

Device-based login is a simple, effective way to control who can access and use particular features on your imageRUNNER ADVANCE device. It also enables you to build a detailed record of usage that can be reviewed when needed.

You can authenticate users with individual or departmental IDs and passwords. You can even leverage Single Sign On (SSO-H) capabilities to allow users to log in with the same passwords used for their PCs.



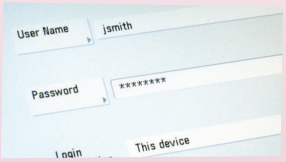
Enter the Dept. ID and PIN using the numeric keys.
(Black copying and printing can be used without entering the Dept. ID and PIN).

Dept. ID: 1234

PIN: ****

Department ID Management Mode

Department ID Management Mode is a built-in imageRUNNER ADVANCE feature that serves as a basic form of device access management for administrators. Department IDs are numeric and are stored locally on the device to let your business control access to the device.



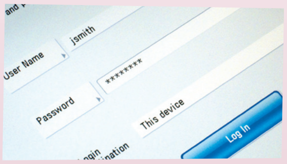
User Name: jsmith

Password: ********

Login: This device

Local Device Authentication

This solution enables you to store usernames and passwords for authorized users locally on the device itself. Once implemented, Local Device Authentication can be set to require that users log in before they can operate the device. Administrators can use a convenient Web-based interface to set up and manage the alphanumeric usernames and passwords.



User Name: jsmith

Password: ********

Login Destination: This device

Single Sign On Login

Single Sign On (SSO-H) is a user authentication function that can be easily integrated with an Active Directory network environment. Leveraging user accounts from Active Directory reduces the burden on network administrators and eliminates the need for users to remember yet another password. SSO-H provides direct authentication using the Kerberos or NTLMv2 protocols.

Card-Based Authentication

Facilitate quick, easy authentication by allowing users to leverage ID cards that may already be implemented for computer login or building access. Card-based authentication systems can be built on a device to work locally or over a network.

Advanced Authentication Proximity Card (Professional Service)

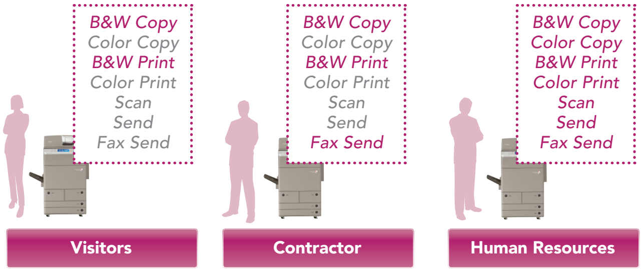
Advanced Authentication Proximity Cards enable support for an optional card reader on imageRUNNER ADVANCE devices. Advanced Authentication Proximity Card is an embedded (serverless) MEAP application that lets you use existing HID proximity ID cards for device access and use. Administrators can leverage IDs stored locally on the device or Active Directory login via SSO-H.

uniFLOW Card-Based Authentication

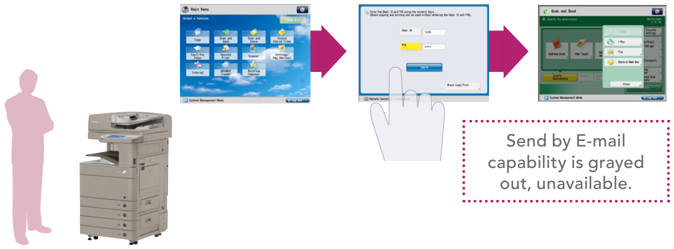
uniFLOW Output Manager is a network-wide print cost control solution that features a robust authentication module. The solution supports a variety of card types such as magnetic cards and HID proximity cards that can be customized to help any business streamline print costs while drastically reducing security concerns.

Manage and Limit User Access According to Job Responsibilities

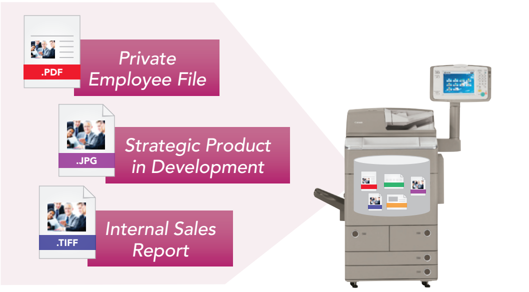
When using the Access Management System, IT administrators can configure imageRUNNER ADVANCE device access for both individuals and groups on a feature-by-feature basis. In fact, the Access Management System's new Function Level Authentication capability can be set to require that users authenticate after selecting certain features, thereby granting or restricting access based on function.



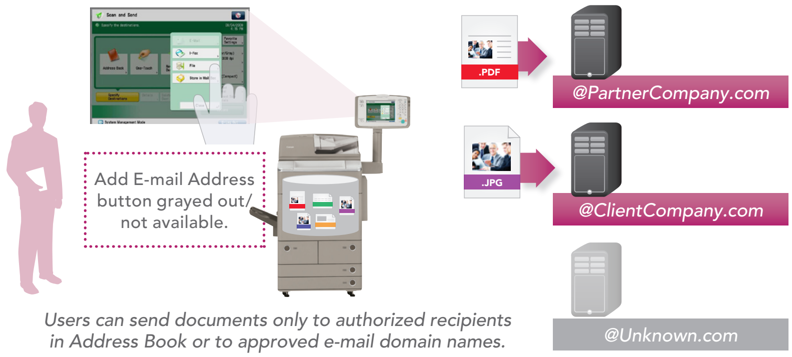
With Access Management System settings in place, after a user authenticates, available features are clearly visible, while restricted features are grayed out.



Function Level Authentication lets you implement settings that restrict specific device capabilities, such as the Send function, by requiring the user to authenticate prior to using those capabilities.



Most companies don't want documents containing confidential information to be e-mailed to unauthorized recipients.



Users can send documents only to authorized recipients in Address Book or to approved e-mail domain names.

Universal Send Destination Restriction

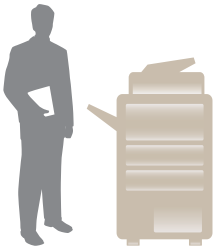
With Universal Send, administrators can limit send capability to preapproved e-mail addresses or domain names only. The feature can also be used to prevent employees from sending documents to specific destinations, and it can also restrict users from adding specific types of new destinations.

Need to reduce risk of sensitive documents being accessed by unauthorized people?

Whenever documents are printed, sent, stored, or exchanged, there may be security concerns. How can you be sure all the information in your documents and workflows is secure?

Can we be sure confidential printouts don't sit in the output tray unattended?

Can we be assured that only authorized users have access to scanned and printed documents?



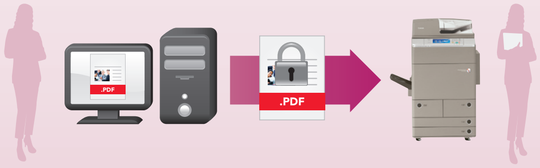
Are there ways to protect incoming faxes from theft or misplacement?

Can we ensure the integrity of the electronic document files we print and send?

Can we track and protect documents after they are printed?

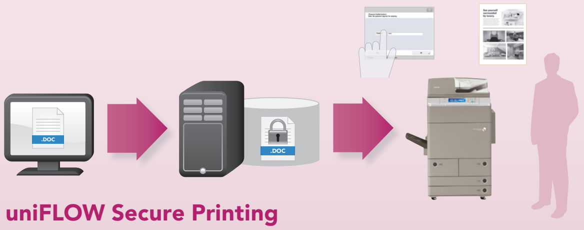
Secure Printing

In offices worldwide, there is always a need to handle sensitive or confidential information. Often that means printing documents with private information, and sometimes that means there is a risk that sensitive documents may be printed out and accidentally left exposed in paper trays. Canon offers several security solutions that help your business reduce risks like these.



Secured Print and Encrypted Secure Print

Secured Print lets users protect documents they send to print. Rather than print automatically, jobs are held securely at the imageRUNNER ADVANCE MFP until released by the user entering the correct password. This step prevents documents from being left out in a device tray unattended. For enhanced security, the document data itself can also be encrypted during transmission and storage when printed with Encrypted Secure Print.



uniFLOW Secure Printing

uniFLOW Output Manager enables you to increase security measures for device activity across your organization. To prevent unauthorized persons from retrieving confidential printouts, jobs can be held at the uniFLOW Output Manager server until a user provides identification at a networked imageRUNNER ADVANCE device. This way any user can print a secure job and then select where to retrieve the document.

Document Storage Space Protection

There are two areas in which documents can be stored and password protected on an imageRUNNER ADVANCE.

Mail Box

imageRUNNER ADVANCE systems offer an onboard secure printing workflow. For example, a user can store print jobs to a password-protected Mail Box on the device. Later, that same user can walk up to the device and enter the Mail Box password to print the job as needed.

Advanced Box

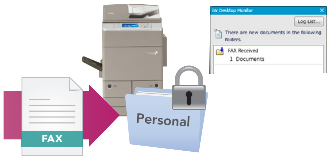
Advanced Box is the collaborative storage space on imageRUNNER ADVANCE systems. Advanced Box enables users to store electronic files within a multitiered folder structure. Folders may be password protected to protect document access. Both native and printable files are accessible from PCs. Printable versions of files are accessible directly from the User Interface at the device.

Fax Forwarding

The Mail Box and Advanced Box each enable you to protect incoming fax documents.

Mail Box Fax Forwarding

Incoming faxes can be set so they are routed to a recipient's personal Mail Box on the imageRUNNER ADVANCE. This way, faxes don't just print out as they arrive. Users can access and print their faxes confidentially if they choose to.

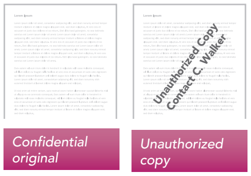


There are new documents in the following folders.

FAX Received
1 Documents

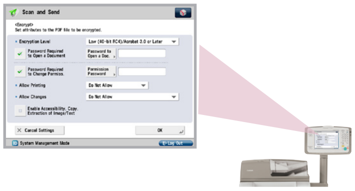
Advanced Box Fax Forwarding

Incoming faxes can be set to automatically route to password-protected Advanced Box folders. When fax documents arrive, a notification may be generated to prompt recipients that a new fax has arrived for them. This way they have the option to retrieve it immediately.



Secure Watermark

You can output your documents with hidden text embedded in the background. If a copy is made, the hidden text appears on the resulting pages, making clear that the copy is unauthorized.



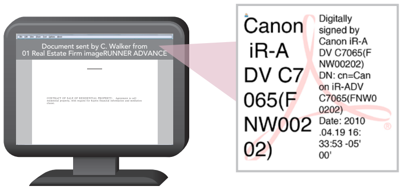
Scan and Send

<Encrypt>
Set attributes to the PDF file to be encrypted.

- Encryption Level: Low (40-bit RC4)/Acrobat 3.0 or Later
- ☑ Password Required to Open a Document — Password to Open a Doc.
- ☑ Password Required to Change Permiss. — Permission Password
- Allow Printing: Do Not Allow
- Allow Changes: Do Not Allow
- □ Enable Accessibility, Copy, Extraction of Image/Text

Password-Protected PDF/XPS

This mode enables the password protection of documents scanned and converted to PDF or XPS on an imageRUNNER ADVANCE system. After the document is distributed by the imageRUNNER ADVANCE device, only those who enter the correct password can open, edit, or print the document.



Document sent by C. Walker from
01 Real Estate Firm imageRUNNER ADVANCE

CONTRACT OF SALE OF RESIDENTIAL PROPERTY: Agreement to sell residential property, with request for buyers financial information and mediation clause.

Canon iR-ADV C7065(FNW00202)

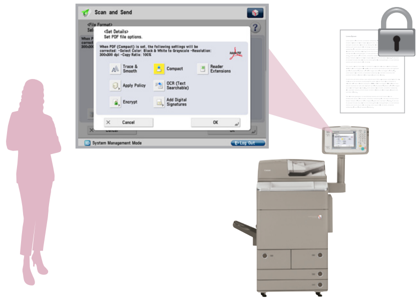
Digitally signed by Canon iR-ADV C7065(FNW00202)
DN: cn=Canon iR-ADV C7065(FNW00202)
Date: 2010.04.19 16:33:53 -05'00'

Digital User Signature and Digital Device Signature

When a hard copy is scanned and converted to a PDF document on an imageRUNNER ADVANCE system, the Digital User Signature PDF kit can be used to embed a digital signature containing that user's name into the document. This confirms the user's identity as the source of the document and facilitates notification if changes are made to it. Device Signature PDF mode embeds the device's serial number in the document in much the same way, enabling the recipient to verify the identity of the original device.

Adobe® LiveCycle® Rights Management

Once you scan and create a PDF, it can easily be distributed. But that doesn't mean you have to give up control over who has access to it or to any sensitive information it might contain. With Canon imageRUNNER ADVANCE devices, you can embed Adobe® LiveCycle® Rights Management ES technology to those PDFs. Whenever users want to open the document, the technology asks them to enter a password that is then checked by an online approvals server. You can set time limits or revoke document privileges at any time.

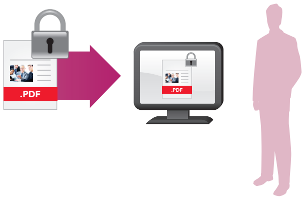


Scan and Send

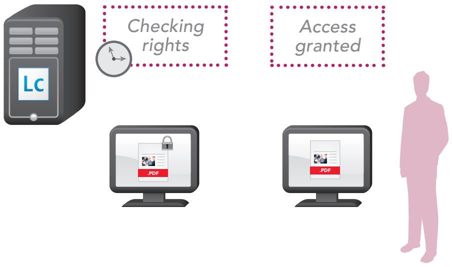
<Set Details>
Set PDF file options.

When PDF (Compact) is set, the following settings will be corrected: -Select Color: Black & White to Grayscale -Resolution: 300x300 dpi -Copy Ratio: 100%

Author saves document with LiveCycle Rights Management policy applied.



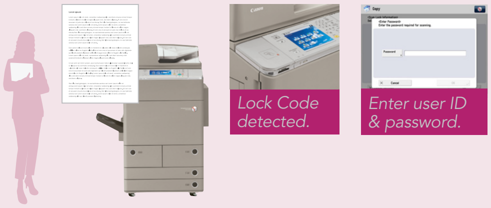
Document is distributed to authorized contractor for a project.



The LiveCycle Rights-managed document checks back with online server before opening.

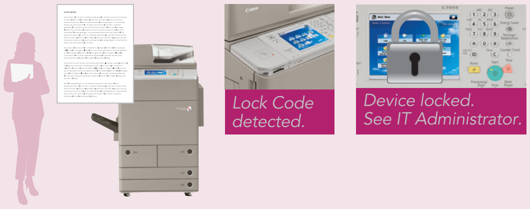
Document Scan Lock/Trace

Document Scan Lock/Trace is a new Canon security technology that enables a business to keep tighter control over its original documents.



Copy

<Enter Password>
Enter the password required for scanning.



An encrypted code can be embedded into hard-copy documents. If a user later tries to copy, scan, or fax one of those hard copies from the same or another networked imageRUNNER ADVANCE system, a variety of security actions can take place, depending on how the encryption was originally set up.

The user can be prompted for an authorized password or user authentication before it will proceed, or the device can lock down, preventing further scanning of the document. In either case, the technology can trace the user that imaged the document and notify a designated administrator.

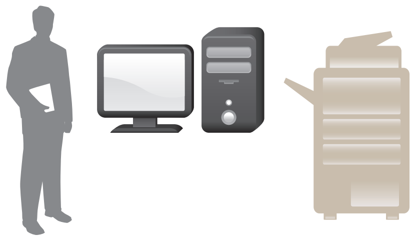
Want to secure the information residing on and transferred through your MFP?

Is unprotected information saved on, or being transferred to, your network print devices leaving your business more vulnerable to threats?

How can we prevent information leaks?

Is it safe to store and share confidential documents on an MFP hard drive?

Are there ways to find out who may have been the source of a critical leak?



Do our security measures help us facilitate compliance?

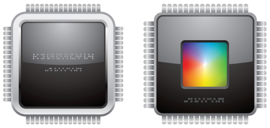
Can standard network security measures be applied to our MFPs?

Data Security

Hard drives on Canon imageRUNNER ADVANCE devices help keep your data secure. As a standard security measure, all data is compressed into a proprietary Canon format written to random, noncontiguous locations on the HDD, while directory data is safely stored separately. These features help ensure that hard drives stay safe, and sensitive information remains confidential.

HDD Data Encryption Kit

The optional HDD Data Encryption Kit, a technology featuring AES 256-bit encryption, ensures that all data stored on the internal disk drive is protected. In recognition of its effectiveness, the kit has received Common Criteria Certification of Evaluation Assurance Level 3 (EAL3).



Trusted Platform Module (TPM)

Canon imageRUNNER ADVANCE MFPs feature a TPM chip that safely stores the encryption key (TPM key) that encrypts confidential information such as passwords, public key pairs for SSL communication, and user certificates that are stored in the device. The technology enables you to protect important information.

10011100011
01001000101
11100011100
01000101010
00011100001
00101010101
11100001111
01010101010
00001111001
MANAGEMENT INFORMATION
ACTUAL DATA

Standard HDD Format

Best practices, and often company policies, usually recommend that systems be completely wiped prior to being redeployed or at the end of their usable lives. The Hard Disk Drive Format feature, which comes standard on every imageRUNNER ADVANCE, completely overwrites all data stored on the hard disk with null data. This includes files, job logs, Address Books, and customized user mode settings.

HDD Data Erase Kit

The optional HDD Data Erase Kit enables administrators to configure their imageRUNNER ADVANCE to overwrite the internal image server hard disk and erase previous data as part of routine job processing. The technology can be set to overwrite once with null data, once with random data, three times with random data, or DoD 5022.22M 3-pass overwrite mode.

Removable HDD

The optional imageRUNNER Removable HDD Kit enables administrators to physically remove the device’s internal hard disk so it can be locked down in a secure place after hours. The drive can then easily be reinstalled for use during normal working hours.

Network Security

Canon imageRUNNER ADVANCE devices include a number of highly configurable network security features designed to help protect your organization's information. Standard features include the ability to permit only authorized users 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 as desired.

Secure Socket Layer (SSL) Encryption

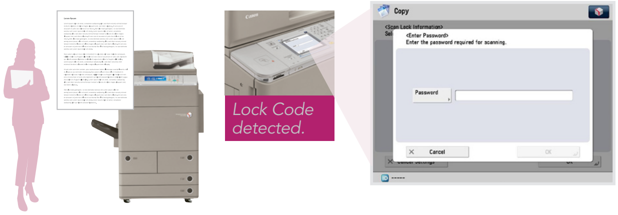
Canon provides Secure Socket Layer (SSL) encryption support for transmissions to and from the imageRUNNER device. Data transmission methods that can use SSL encryption include IPP, Internet-fax, Remote UI, and WebDAV.

Mac Address Filtering and IP Address Filtering

MAC and IP address filters can be used to allow or deny access to specific device or machine addresses. Administrators can manage addresses using the Remote UI interface and can limit access to imageRUNNER ADVANCE devices with individual or consecutive IP addresses or ranges. Also, a range of IP addresses can be permitted while certain addresses within that range are rejected.

Tracking and Auditing

Canon offers various solutions that will continuously capture, archive, and audit device activity information. Details that can be captured include IP addresses, job type, time, date, and user. More advanced solutions can capture text and images of document pages. In the event of a security breach, this information can be searched through, accessed, and reviewed.



Lock Code detected.

Copy

<Scan Lock Information>

<Enter Password>
Enter the password required for scanning.

Document Scan Lock/Trace Auditing

imageRUNNER ADVANCE systems enable you to see a detailed summary of activity on any document that is copied or scanned if it has imageRUNNER ADVANCE lock code information embedded within it.

imageWARE Secure Audit Manager

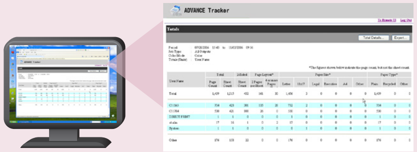
Canon's imageWARE Secure Audit Manager is a robust network device security solution that delivers detailed oversight of your company's document-related activities. It is able to capture, archive, and audit the activities that occur on Canon devices, including storing a complete, searchable image of every document. By constantly monitoring device-related activities, imageWARE Secure Audit Manager deters potential wrongdoers from leaking important and valuable information. If leaks do occur, the system automatically logs and distributes actionable intelligence to administrators.

imageWARE ADVANCE Tracker and imageWARE Enterprise Management Console Plug-in

Although primarily created for cost control functionality, imageWARE Accounting Manager for MEAP and imageWARE Enterprise Management Console Accounting Management Plug-in also provide a detailed audit trail of device activities for security purposes.

Tracker generates activity logs that can provide insight into how each employee is using a single device.

The imageWARE Enterprise Management Console Accounting Management Plug-in gives you a complete record of user activity on all network output devices from one Web-based location.



Monitor print activity through a Web-based tool, or have reports e-mailed to you automatically.

Scale Up As You Grow

Every company has different security needs. That's why Canon offers a wide variety of security solutions that you can choose from. If needed, you can get started with the basic security measures included in every imageRUNNER ADVANCE device. As your company or its needs grow, you can easily add additional systems and solutions.

Meeting the Unique Output Needs of Your Business

In an era of relentless competition, business leaders look for solutions that simplify and improve critical processes within their infrastructures. Canon stands ready to offer in-depth knowledge, practical expertise, and field-tested technology when developing solutions for all your document-related challenges.

Whether you're considering hardware, software, or both, Canon Professional Services can help your team analyze and evaluate your existing processes, then partner with you to carefully implement integrated solutions linked to your business goals.

LET YOUR BUSINESS RUN

COLOR · DOCUMENT MANAGEMENT · DOCUMENT DISTRIBUTION · PRODUCTIVITY · SECURITY

COST RECOVERY · DEVICE MANAGEMENT · USABILITY · ACCESSIBILITY · ENVIRONMENT

Canon
imageANYWARE

CANON and IMAGERUNNER are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. IMAGEANYWARE is a trademark of Canon. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.

Regulatory Disclaimer
Statements made in this document are the opinions of Canon U.S.A. None of these statements should be construed as legal advice, as Canon U.S.A. does not provide legal counsel or compliance consultancy, including without limitation, Sarbanes Oxley, HIPAA, GLBA Check 21, or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Products shown with optional accessories/equipment. The features reviewed in this brochure include both standard and optional solutions for IMAGERUNNER ADVANCE systems. Specifications and availability subject to change without notice.

0310-SEC3-2M-KC

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

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