



MFD HARDENING GUIDE

imageRUNNER ADVANCE

Canon



INTRODUCTION

Modern Canon Multifunction Devices (MFDs) provide print, copy, scan, send and fax functionality. MFDs are computer servers in their own right, providing a number of networked services along with significant hard drive storage.

When an organisation introduces these devices into their infrastructure, there are a number of areas that should be addressed as part of the wider security strategy, which should look to protect the confidentiality, integrity and availability of your networked systems.

Clearly, deployments will differ and organisations will have their own specific security requirements. While we work together to ensure that Canon devices are shipped with appropriate initial security settings, we aim to further support this by providing a number of configuration settings to enable you to more closely align the device to the requirements of your specific situation.

This document is designed to provide sufficient information to enable you to discuss with Canon or Canon partner the most appropriate settings for your environment. It should be noted that not all device hardware has the same level of capability and different system software may provide different functionality. Once decided, the final configuration can be applied to your device or fleet. Please feel free to contact Canon or a Canon partner for further information and support.



Who is this document meant for?

This document is aimed at anybody who is concerned with the design, implementation and securing of office multifunction devices (MFDs) within a network infrastructure. This might include IT and network specialists, IT security professionals, and service personnel.

Scope and coverage

The guide explains and advises on the configuration settings for two typical network environments, so that organisations can securely implement an MFD solution based on best practice. It also explains (from system software platform version 3.8) how Syslog functionality can provide real-time feedback from the MFD. These settings have been tested and validated by Canon's Security team.

We make no assumptions about specific industry sector regulatory requirements that may impose other security considerations and are out of scope of this document.

This guide was created based upon the typical feature set of the imageRUNNER ADVANCE platform, and while the information here applies to all models and series within the imageRUNNER ADVANCE range, some features may differ between models.

Implementing appropriate MFD security for your environment

To explore the security implications of implementing a multifunction device as part of your network, we have considered two typical scenarios:

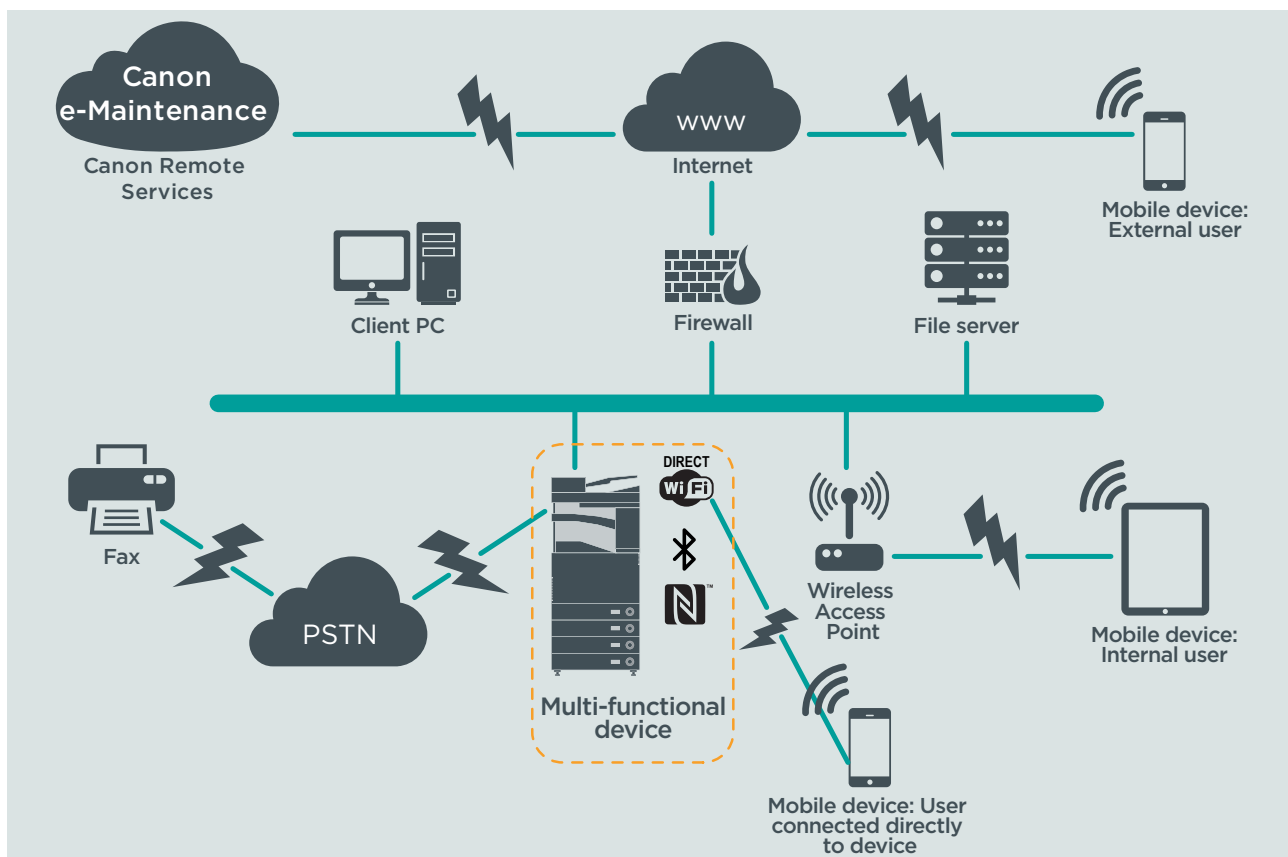
- **A typical small office environment**
- **An enterprise office environment**

SMALL OFFICE ENVIRONMENT

Typically, this will be a small business environment with an un-segmented network topology. It uses one or two MFDs for its internal use and these devices are not accessible on the Internet.

While mobile printing is available, additional solution components will be required. For those users requiring printer services outside of a LAN environment, a secure connection is required, but this will not be covered in this guide. However, attention should be paid to the security of the data in transit between the remote device and the print infrastructure.

Figure 1 Small Office Network



The latest generation of imageRUNNER ADVANCE models provide wireless network connectivity allowing the device to connect to a WiFi network. It can also be used to establish a point-to-point WiFi Direct connection with a mobile device without the need for a network connection.

Bluetooth and NFC options are available for several device models and are used to establish the WiFi Direct connection for iOS and Android devices respectively only.

CONFIGURATION CONSIDERATIONS

Please note that unless a feature of the imageRUNNER ADVANCE is mentioned below, it is regarded as being sufficient in the default settings for this business and network environment.

Table 1 Small Office Environment Configuration Considerations

| ImageRUNNER ADVANCE Feature | Description | Consideration |
|--|---|---|
| Service Mode | Allows access to Service Mode settings | Password protect with a non-default, non-trivial and maximum length password |
| Service Management System | Allows access to various non- standard device settings | Password protect with a non-default, non-trivial and maximum length password |
| SMB Browse/Send | Store and retrieve to and from Windows /SMB network shares | System administrators should, by policy, disallow any users from creating local accounts on their client machine for use in sharing documents with the imageRUNNER ADVANCE over SMB |
| Remote UI | Web-based configuration tool | The imageRUNNER ADVANCE administrator should enable HTTPS for the remote UI and disable HTTP access. Enable the use of PIN authentication unique to each device |
| SNMP | Network monitoring integration | Disable version 1 and enable version 3 only |
| Send to e-mail and/or IFAX | Send emails from the device with attachments | Enable SSL Do not use the POP3 authentication before SMTP send Use SMTP authentication |
| POP3 | Automatically fetch and print documents from mailbox | Enable SSL Enable POP3 authentication |
| Address book / LDAP | Use directory service to look up home number or email addresses to send scans to | Enable SSL Do not use domain credentials to authenticate against the LDAP server; use LDAP specific credentials |
| FTP Print | Upload & download documents to and from the embedded FTP server | Turn on FTP authentication. Be aware that FTP traffic will always travel in clear text over the network |
| WebDAV Send | Scan and Store documents on a remote location | Enable authentication for WebDAV shares |
| Encrypted PDF | Encrypt documents | By policy sensitive documents should only be encrypted using PDF version 1.6 (AES-128) |
| Secure Print | Print job is sent to the device but locked in the print queue until the corresponding PIN number is entered | Enable PIN protected print jobs |
| Syslog event notification | System Logging Protocol is a standard industry protocol used to send system log or event messages to a specific server called a Syslog server | Consider pointing the imageRUNNER Syslog data to your existing network syslog analysis tool or enterprise Security Event Management System (SIEM) platform. |
| Verify System at start-up | Provides assurance that the system software components have not been compromised. It will have a minimal impact upon system boot time | Enable function |
| Embedded web browser | Browser access to Internet | Enforce through administration, the use of a content filtering web proxy to avoid malicious or viral content being accessed. Disable the creation of favourites |
| Bluetooth and NFC (available from Generation 3 models) | Used to establish a WiFi Direct connection | Enable WiFi Direct to allow direct connection to a mobile device. WiFi Direct may not be used when WiFi is used to connect to a network |
| Wireless LAN | Provides Wireless access | Use WPA-PSK/WPA2-PSK with strong passwords |
| IPP | Connect and send printing jobs over IP | Disable IPP |
| TPM | A feature that stores security data, such as passwords and encryption keys, in hardware to ensure maximum protection | This feature is off by default. When enabled, it is recommended that a backup is created |



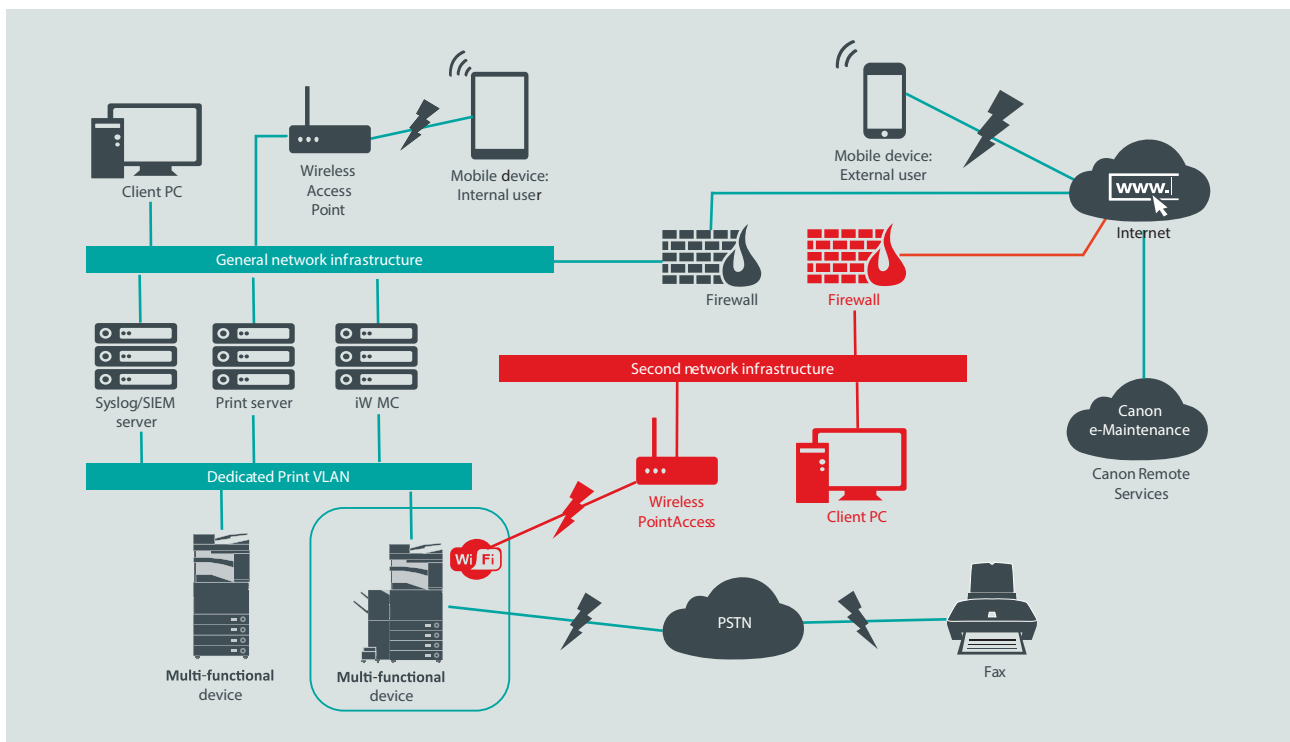
AN ENTERPRISE OFFICE ENVIRONMENT

This is typically a multi-site, multi-office environment with segmented network architecture. It has multiple MFDs deployed on a separate VLAN accessible for internal use via print server(s). These MFDs are not accessible from the Internet.

This environment will usually have a permanent team to support its networking and back office requirements along with general computer issues, but it is assumed they will not have specific MFD training.

This is typically a multi site, multi office environment with segmented network architecture. It has multiple MFDs deployed on a separate VLAN accessible for internal use via print server(s). These MFDs are not accessible from the Internet.

Figure 2 Enterprise Office work



Connections highlighted in red will be available from Generation 3 models

CONFIGURATION CONSIDERATIONS

Please note that unless a feature of the imageRUNNER ADVANCE is mentioned below it is regarded as being sufficient in the default settings for this business and network environment.

Table 2 Enterprise Office Environment Configuration Considerations

| imageRUNNER ADVANCE Feature | Description | Consideration |
|---|---|--|
| Service Mode | Allows access to Service Mode settings | Password protect with a non-default, non-trivial and maximum length password |
| Service Management System | Allows access to various non- standard device settings | Password protect with a non-default, non-trivial and maximum length password |
| SMB Browse/Send | Store and retrieve to and from Windows /SMB network shares | System administrators should, by policy, disallow any users from creating local accounts on their machine for use in sharing documents with the imageRUNNER ADVANCE over SMB |
| Remote UI | Web-based configuration tool | Following initial device configurations disable the Remote UI completely by disabling HTTP and HTTPS |
| SNMP | Network monitoring integration | Disable version 1 and enable version 3 only |
| Send to e-mail and/or IFAX | Send emails from the device with attachments | Enable SSL Enable: - Certificate verification at the SMTP server Or if not viable: - Only use this feature in an environment where a Network Intruder Detection System collector is present Do not use the POP3 authentication before SMTP send Use SMTP authentication |
| POP3 | Automatically fetch and print documents from mailbox | Enable SSL Enable: - Certificate verification at the POP3 server Or if not viable: - Only use this feature in an environment where a Network Intruder Detection System collector is present Enable POP3 authentication |
| Address book / LDAP | Use directory service to look up phone number or email addresses to send scans to | Enable SSL Enable: - Certificate verification at the LDAP server Or if not viable: - Only use this feature in an environment where a Network Intruder Detection System collector is present Do not use domain credentials to authenticate against the LDAP server; use LDAP specific credentials |
| IPP | Connect and send printing jobs over IP | Disable IPP |
| WebDAV Send | Scan and Store documents on a remote location | Enable authentication for the WebDAV shares Enable SSL Enforce the printer to only allow files ending with the "file printing extensions" to be uploaded |
| IEEE802.IX | Network access authentication mechanism | EAPOL V1 supported |
| Encrypted PDF | Encrypt documents | By policy sensitive documents should only be encrypted using PDF version 1.6 (AES-128) |
| Encrypted Secure Print | Enhance the protection of Secure Print by encrypting the file and the password during transmission | Configure the username in the Printer tab on the client printer configuration to a different username than the LDAP/domain credentials of that user. Ensure "Restrict printer jobs" is turned off |
| Certificate Auto Enrolment | The auto enrolment process improves the efficiency of digital certification retrieval and deployment | Requires a network certificate solution to leverage |
| Syslog event notification | System Logging Protocol is a standard industry protocol used to send system log or event messages to a specific server called a Syslog server | Consider pointing the imageRUNNER ADVANCE Syslog data to your existing network syslog analysis tool or enterprise Security Event Management System (SIEM) platform |
| Verify System at start-up | Provides assurance that the system software components have not been compromised. It will have a minimal impact upon system boot time | Enable function |
| Wireless LAN | Provides Wireless access | Use WPA-PSK/WPA2-PSK with strong passwords |
| WiFi Direct | Used to establish a WiFi Direct connection | Disable WiFi Direct |
| Embedded web browser (available from Generation 3 2nd edition models) | Browser access to Internet | Apply appropriate restrictions or disable ability to download files acquired via the browser |

The latest generation of imageRUNNER ADVANCE models provide wireless network connectivity allowing the device to connect to a WiFi network whilst simultaneously connected to a wired network. This scenario can be useful where the customer needs to share a device across two networks. A school environment is a typical example where there are separate staff and pupil networks.

The imageRUNNER ADVANCE platform provides a feature environment to allow for flexible use. With the protocols and services available to achieve this, it is important to ensure that only the required features, services and protocols are enabled to fulfil the needs of the user. This is good security practice and will reduce the potential attack surface and prevent their exploitation. As new vulnerabilities are constantly appearing we must always be vigilant to compromising, either intrinsically or extrinsically to the device. Having the ability to monitor user activity is useful to help identify and take corrective action when needed.

imageRUNNER ADVANCE software platform version 3.8 provides some additional features to those that have been available for a number of years. These include the ability to monitor the device in real-time using Syslog and Verify System at Start-Up. Using these features in collaboration with your existing network security solutions, such as a Security Information Event Management platform or logging solution, allows for wider visibility and the identification of incidents and for forensic purposes.

Trusted Platform Module (TPM)

Every imageRUNNER ADVANCE device includes a Trust Platform Module (TPM) which is a temper-resistant open standard security chip (imageRUNNER ADVANCE DX models are equipped with TPM 2.0). It is responsible for the storage of passwords, digital certificates and cryptographic keys.

All current imageRUNNER ADVANCE models with hard disk or solid state drives provide full-drive encryption the encryption key for which is stored are stored in the Canon MFP Security Chip, which complies with FIPS 140-2 Level 2 security standard (established by the United States Government), and not the TPM.

As a default, the TPM functionality is disabled; however, it can be enabled by accessing the imageRUNNER ADVANCE Additional Functions menu. It is strongly recommended the TPM is backed up in the event of failure immediately after it has been enabled. It should be noted that it can only be backed once to a USB memory stick.

For further information related to the TPM, point your web browser to the link below and enter Using TPM in the search box. This will give information related to:

- Activating the TPM
- Backing up and restoring the TPM

<https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/>



Verify System at Start-Up

This functionality is a hardware mechanism which is designed to ensure that all parts of the imageRUNNER ADVANCE Generation 3 3rd edition system software are verified against a Root of Trust to ensure that the operating system loads as Canon intends. Should a malicious party tamper, try to modify the system or should there be an error loading the system, the process will stop and an error code displayed.

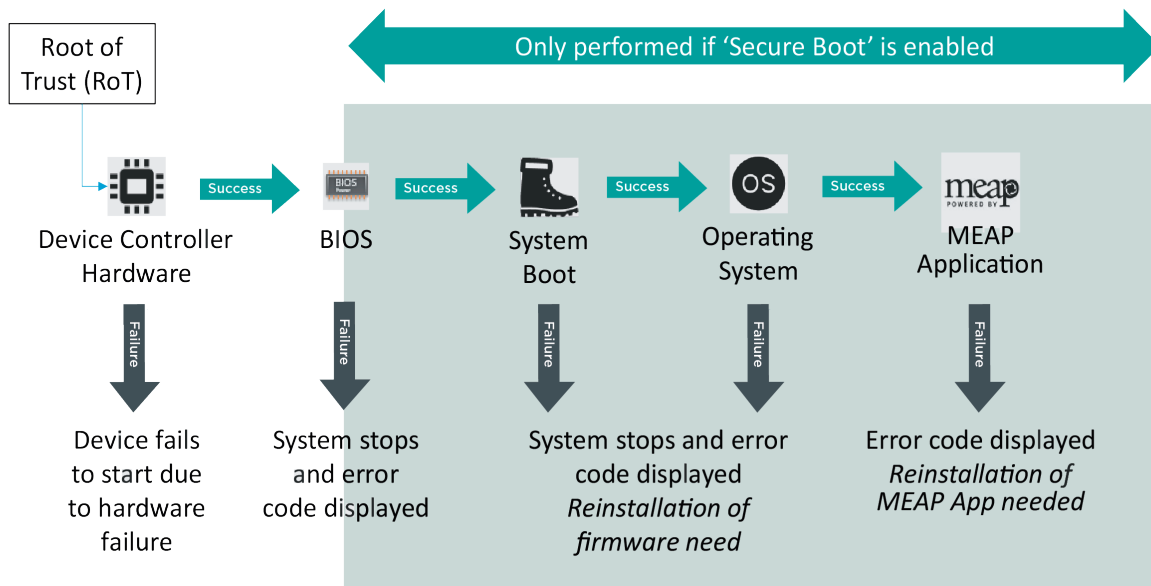


Figure 3 Verify System at Start-Up process

This process is transparent to the user apart from the display indicating an unintended system version being loaded. The imageRUNNER ADVANCE Generation 3 3rd edition has an option to enable Verify System at Start-Up which should be switched on to enable this security feature.

Secure Data Erase

The multi-functional device handles data to perform copy, scan, print and fax jobs as well as address books, system logs and job history which could ultimately contain sensitive information. The imageRUNNER ADVANCE platform provides a secure data erase function to ensure that not just the file allocation table entry for the deleted data is removed but the sectors storing data are overwritten with dummy data preventing any recovery.

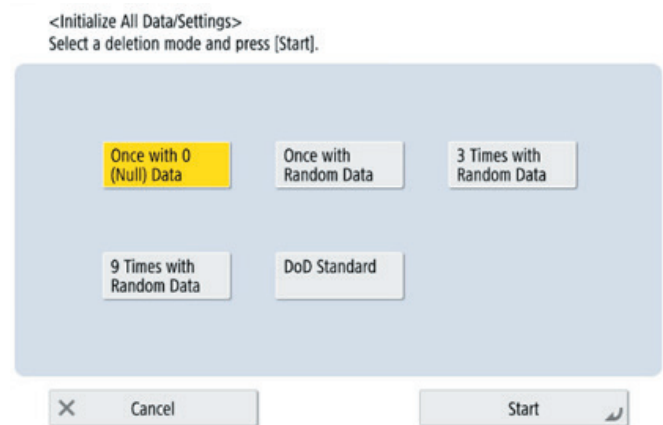


Figure A: Data overwrite options for HDD equipped imageRUNNER ADVANCE

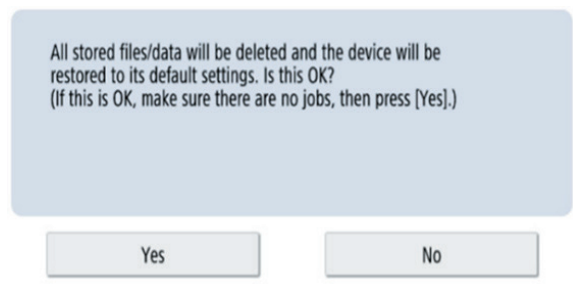


Figure B: Initialise all SSD data for imageRUNNER ADVANCE

Depending upon the specific model of device, either a hard disc drive (HDD) or solid-state drive (SSD) is used. As an HDD uses a physical spinning platter on which data is recorded, a number of overwrites, generally three, are required to ensure that an effective overwrite is performed. However, SSD technology manages storage differently by distributing memory allocation evenly across the whole available space making the need to overwrite multiple time unnecessary.

SSD Technology

Unlike an HDD, with an SSD there should not be the need to perform maintenance as self-sufficiency has been built-in by design by using algorithms and fail-safes to ensure data is discarded efficiently whilst maximising lifespan. Data is stored electrically in solid-state memory cells, which has the benefit of speed of access but the problem of each cell only having a finite number of writes.

Wear Levelling

To counter the issue of excessive wear to a particular memory block, a process known as Wear Levelling is employed to ensure the number of writes kept as even as possible. Two principles are used: dynamic wear levelling and static wear levelling.

Dynamic wear levelling allocates storage blocks so that rewrites are repositioned to new empty blocks. A wear counter is then incremented to allow the SSD controller to keep track of wear. Static wear levelling takes the approach of moving existing unmodified data to a new memory block thereby spreading wear more evenly across the available storage. The principle is to distribute the number of rewrites evenly across all memory blocks irrespective as to where the data only changes occasionally or constantly. The 'TRIM' process helps to contribute towards extending life and ensuring high-speed data mapping.

Depending upon the imageRUNNER ADVANCE model, several different configuration options which can be configured to set the point at which an overwrite is performed and the overwrite method. Models which used HDD storage previously provided a complete data deletion function to completely erase data.

- SSD is encryption key is stored in the specific device - if removed from the specific device, data is encrypted using **AES 256-bit** and cannot be read/written
- Canon MFP Security Chip 2.10 complies with the **FIPS 140-2 Level 2** (U.S. government standard)

Initialize All Data/Settings

- **Limited to [Once with 0 (Null) Data]**
- SSD is solid-state and HDD uses spinning magnetic discs.
- Also, after writing once with 0 data, it is virtually impossible to read the data written because the access table is rewritten, the location of the data is unknown.
- Since the stored data is encrypted, it is not possible to read/write data on a PCs or after installation on a different MFP.

Certificate Auto Enrolment

In imageRUNNER ADVANCE system software platform versions prior to version 3.8, the administrator had to manually install updated security certificates on each device. This is a laborious task as there is the need to connect to each device in turn to perform a manual update – certificates must be installed manually using the specific device Remote User Interface (RUI) making the process much more time consuming. With the Certificate Auto Enrolment Service introduced from platform version 3.8 and above, this overhead has been eliminated.

The auto enrolment process improves the efficiency of certification retrieval. It provides the ability to automatically retrieve certificates using the Network Device Enrolment Service (NDES) for Microsoft Windows and Simple Certificate Enrolment Protocol (SCEP).

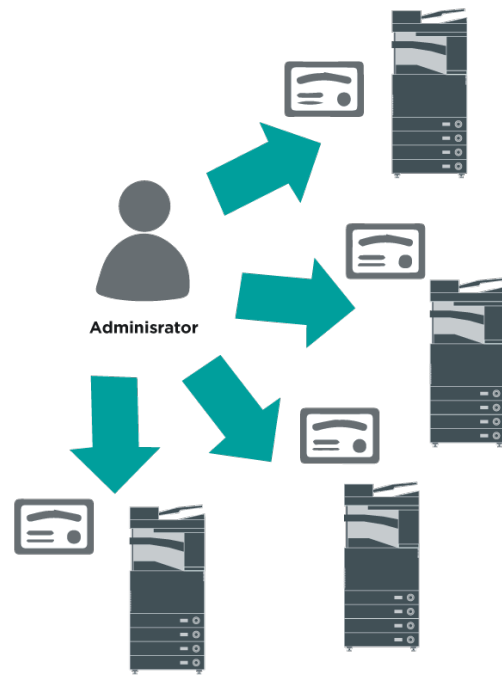


Figure 4 Certificate enrolment

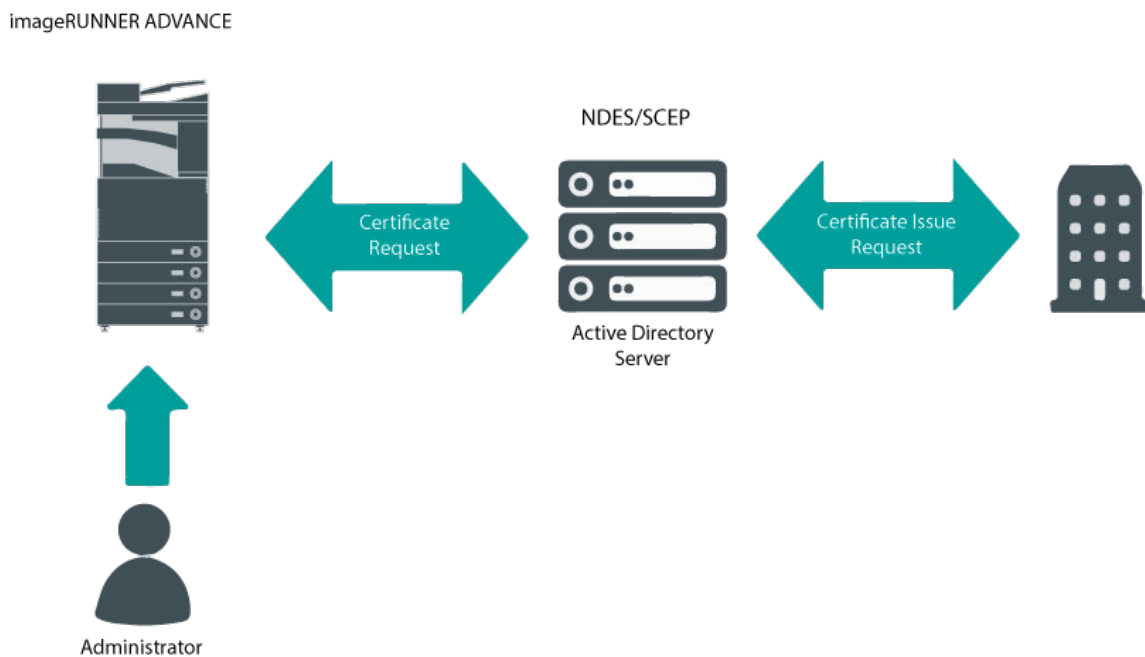


Figure 5 Certificate enrolment process

SCEP is a protocol that supports certificates issued by a Certificate Authority (CA) and NDES enables network devices to retrieve or update certificates based on SCEP.

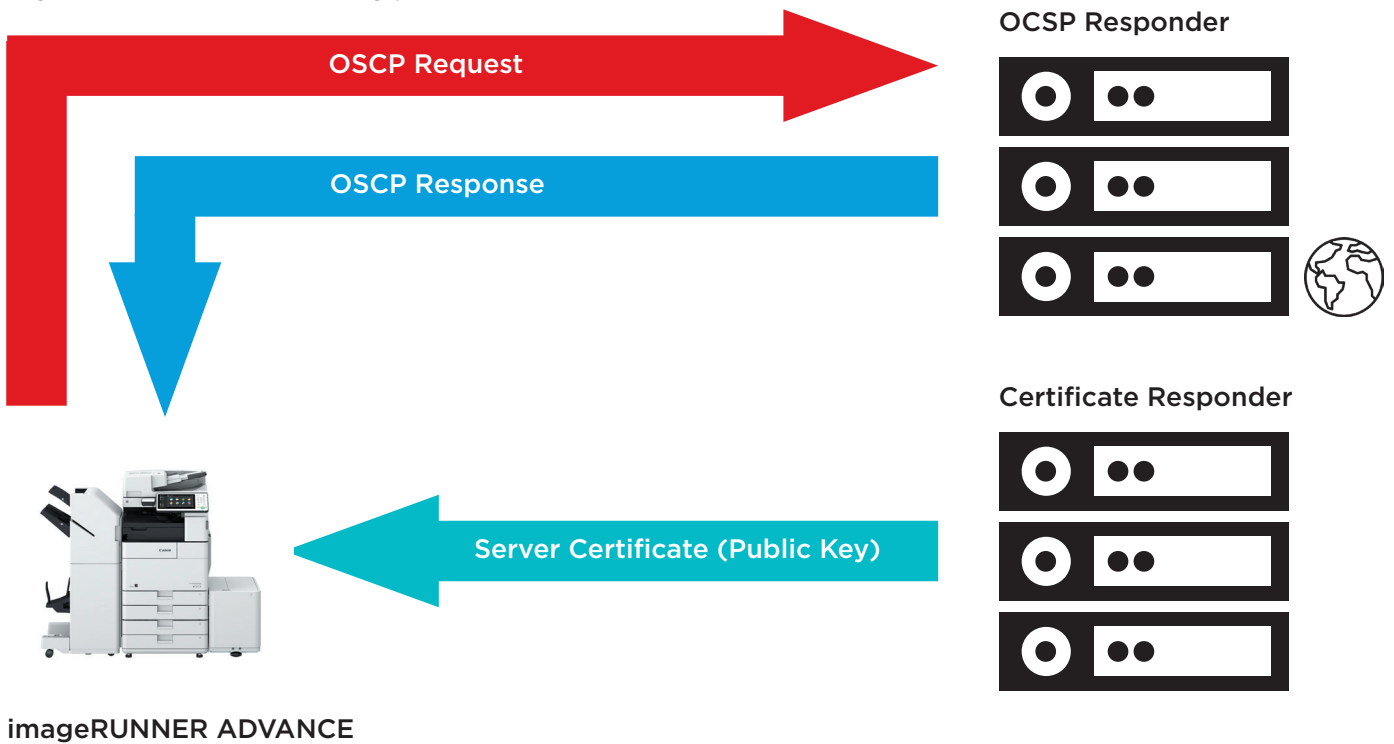
NDES is a role service of the Active Directory Certificate Services.

Online Certificate Status Protocol

There are a number of reasons why it may be necessary to revoke a digital certificate. Examples for this can include the private key has been lost, stolen, compromised or a domain name has been changed.

The Online Certificate Status Protocol (OCSP) is a standard Internet protocol that is used for checking the revocation status of an X.509 digital certificate that has been provided by the Certificate Server. By sending an OCSP Request to the OCSP Responder (typically a certificate issuer) specifying a specific certificate, the OCSP Responder will reply with a 'good', 'revoked' or 'unknown'.

Figure 6 OCSP hand shaking process



With imageRUNNER ADVANCE from Platform version 3.10, OCSP provides a real-time mechanism to verify the installed X.509 digital certificates. Earlier Platform versions only supported Certificate Revoke List (CRL) method which are inefficient and result in heavy overhead on network resources.

Security Information and Event Management

The imageRUNNER ADVANCE technology supports the ability to push out real-time security events using the Syslog protocol which adheres to RFC 5424, RFC 5425 and RFC 5426.

This protocol is used by a wide-range of device types as a way of collecting real-time information that can be used to identify potential security issues.

To facilitate the detection of threats and security incidents, the device must be configured to point to a third-party Security Incident Event Management (SIEM) server.

Syslog events produced by the device can be used to create actions through the real-time collection and analysis of events from a wide variety of contextual data sources (Figure 7). It can also support compliance reporting and incident investigation through the use of additional solutions such as a SIEM server. An example can be seen in figure 8.

The latest generation of imageRUNNER ADVANCE devices provide Syslog functionality that support a range of events that can be collected. This can be used to correlate and analyse events across a number of disparate sources to



Figure 7 Syslog data capture

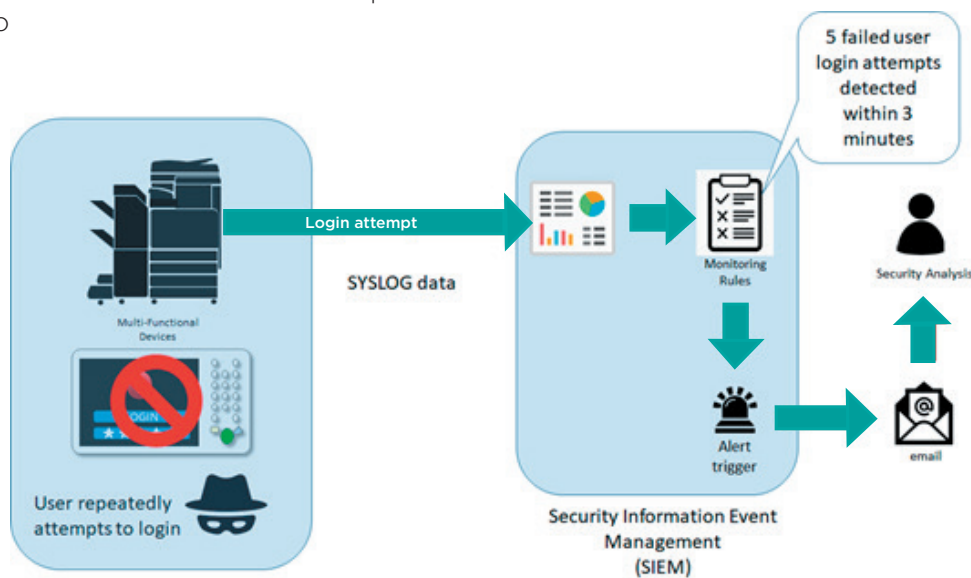


Figure 8 imageRUNNER ADVANCE Syslog data use example

For the list of SIEM operation targets, please point your web browser to the following link and download the “SIEM_spec (imageRUNNER ADVANCE)”.

<https://www.canon.co.uk/support/product-specific-security-measures/>



Device Log Management

In addition to the Syslog functionality provided from system software platform version 3.8, the imageRUNNER ADVANCE has following logs that can be managed on the device. These logs can be exported in CSV file format through the Remote User Interface (RUI).

Table 3 – Examples of log files that can be managed by the multifunctional device.

| Log Type | Number Indicated as “Log Type” in the CSV File | Description |
|--|--|--|
| Log | 4098 | This log contains information related to the authentication status of user authentication (login/logout and user authentication success/failure), the registering/changing/deleting of user information managed with User Authentication, and the management (adding/editing/deleting) of roles with the ACCESS MANAGEMENT SYSTEM |
| Job Log | 1001 | This log contains information related to the completion of copy/fax/scan/send/print jobs |
| Transmission Log | 8193 | The log contains information related to transmissions |
| Advanced Space Save Log | 8196 | This log contains information related to the saving of files to the Advanced Space, Network (Advanced Space of other machines), and Memory Media |
| Mail Box Operation Log | 8197 | This log contains information related to the operations performed on data in the Mail Box, the Memory RX Inbox, and the Confidential Fax Inbox |
| Mail Box Authentication Log | 8199 | This log contains information related to the authentication status of the Mail Box, the Memory RX Inbox, and the Confidential Fax Inbox |
| Advanced Space Operation Log | 8201 | This log contains information related to data operations in the Advanced Space |
| Machine Management Log | 8198 | This log contains information related to the starting/shutting down of the machine, changes made to the settings by using the (Settings/Registration), changes made to the settings by using the Device Information Delivery function, and the time setting The Machine Management Log also records changes in user information or security-related settings when the machine is inspected or repaired by your local authorized Canon dealer |
| Network Authentication Log | 8200 | This log is recorded when IPSec communication fails |
| Export/Import All Log | 8202 | This log contains information related to the importing/exporting of the settings by using the Export All/Import All function |
| Mail Box Backup Log | 8203 | This log contains information related to backups of data in the User Inboxes, the Memory RX Inbox, the Confidential Fax Inbox, the Advanced Space, plus any held data, and the form registered for the Superimpose Images function |
| Application/Software Management Screen Operation Log | 3101 | This is an operation log for SMS (Service Management Service), software registration/updates, and MEAP application installers, etc |
| Security Policy Log | 8204 | This log contains information related to the setting status of the security policy settings |
| Group Management Log | 8205 | This log contains information related to the setting status (registering/editing/deleting) of the user groups |
| System Maintenance Log | 8206 | This log contains information related to firmware updates and backup/restoration of the MEAP application, etc. |
| Authentication Print Log | 8207 | This log contains information and the operation history related to the forced hold print jobs |
| Setting Synchronization Log | 8208 | This log contains information related to the synchronization of machine settings. Synchronizing Settings for Multiple Canon Multifunction Printers |
| Log for Audit Log Management | 3001 | This log contains information related to the starting and ending of this function (the Audit Log Management function), as well as the exporting of logs, etc |

Logs can contain up to 40,000 records. Once the number of records exceeds 40,000, the oldest records are deleted first.

REMOTE DEVICE SUPPORT

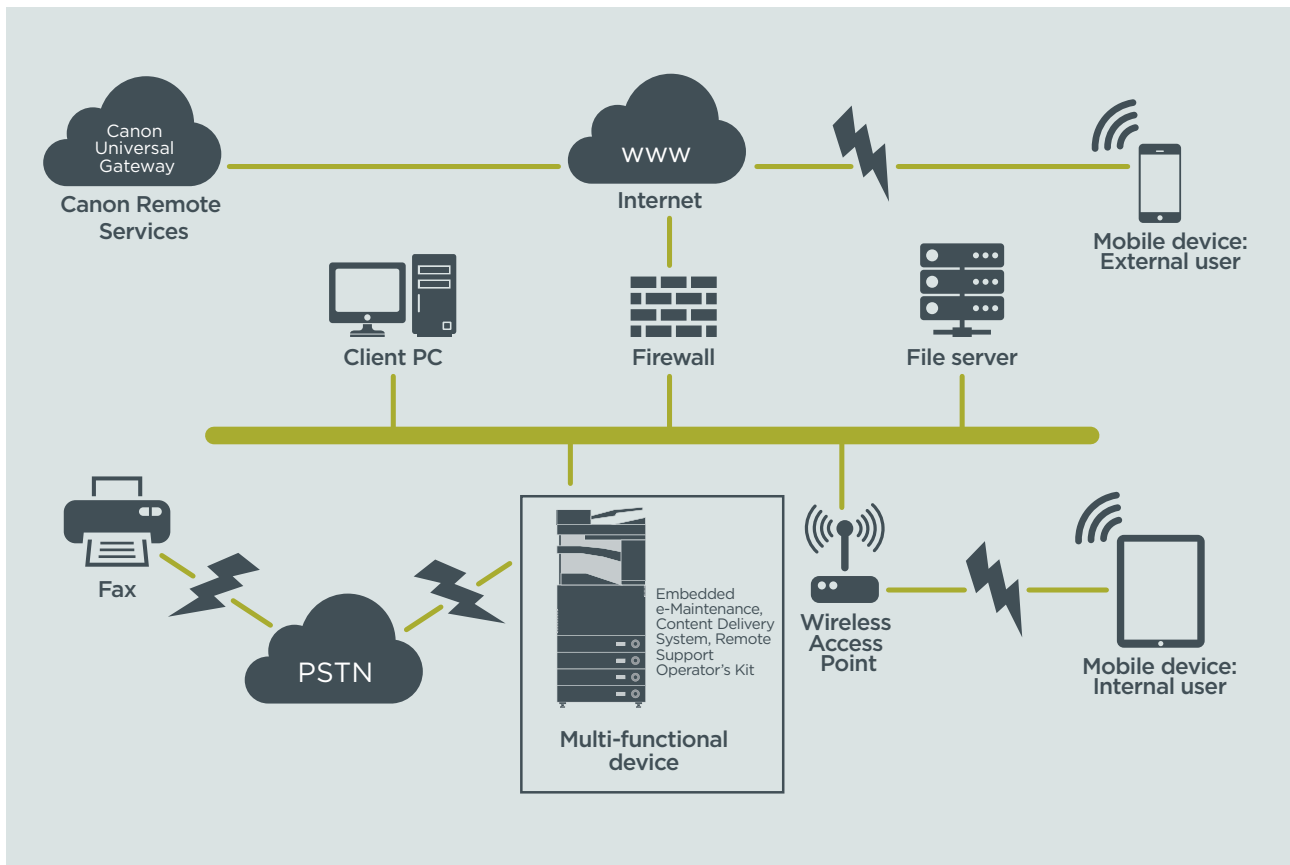
For Canon or a Canon Partner to be able to provide efficient service, the imageRUNNER ADVANCE is capable of transmitting service related data, as well as receiving firmware updates or software applications. It should be noted that no image or image metadata is sent.

Shown below are two possible implementations of Canon's remote services within a company network.

Implementation scenario 1: Dispersed connection

In this setting, each MFD allows direct connection to the remote service through the Internet.

Figure 9 Dispersed connection



Implementation Scenario 2: Centralised Managed Connection

In an enterprise environment scenario, where multiple MFDs are installed, there is a need to be able to efficiently manage these devices from one central point, and this includes the connection to Canon's remote services. To facilitate the holistic management approach, individual devices would establish management connections through a single iW Management Console (iWMC) connection point. For communication between the Device Firmware Upgrade (DFU) plug-in and Multi-Functional Devices, UDP port 47545 is used.

Figure 10 Centralized managed connection

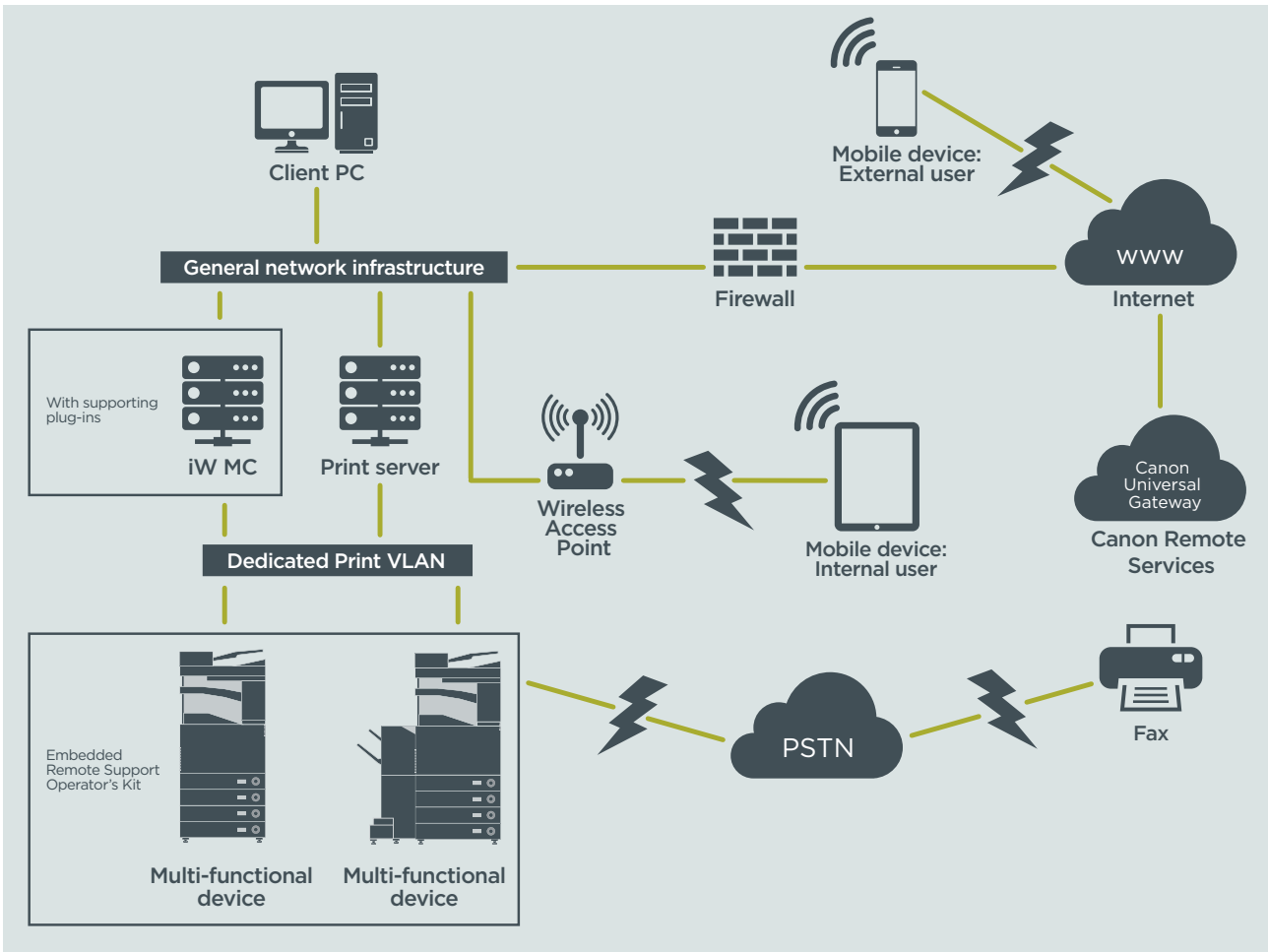


Figure 11a. Device list (in this case a single device) as reported on imageWARE Management Console and 11b. Device details and settings

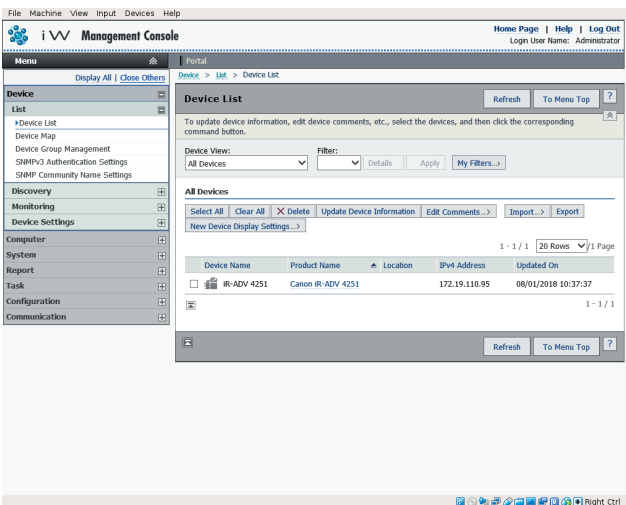


Figure 11a

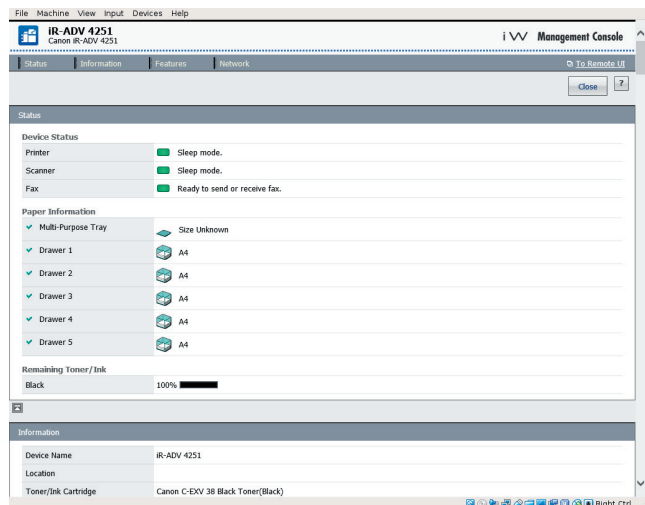


Figure 11b

e-Maintenance

The e-Maintenance system provides an automated way of collecting device usage counters for billing purposes, consumables management and remote device monitoring through status and error alerts.

The e-Maintenance system consists of an Internet facing server (UGW) and either an embedded Multi-Functional Device software (eRDS) and/or additional server-based software (RDS plug-in) to collect device service related information. The eRDS is a monitoring program which runs inside the imageRUNNER ADVANCE. If the monitoring option is enabled in the device settings, the eRDS

obtains its own device information and sends it to the UGW. The RDS plug-in is a monitoring program which is installed in a general PC, and can monitor 1 to 3000 devices. It obtains the information from each device via the network and sends it to the UGW.

As shown in Table 4 below, the next page overviews the data transferred, protocols (depends upon options selected during the design and implementation) and ports used. At no point is any copy, print, scan or fax image data transferred.

Table 4 E-Maintenance Data Overview

| Description | Data Handled | Protocol/Port | Port |
|--|--|--|---|
| Communication between eMaintenance (eRDS or RDS plug-in) and UGW | UGW web service address Proxy server address / port number Proxy account / password UGW mail destination address | HTTP/HTTPS/SMTP/POP3 | TCP/80 TCP/443 TCP/25 TCP/110 |
| Communication between eMaintenance and Device (only RDS plug-in, as eRDS is embedded software) | SMTP server address POP server address Device status, counter and model information Serial number Remaining toner/Ink information Firmware information Repair request information Logging information Service call Service alarm Jam Environment Condition log | SNMP Canon proprietary SLP/SLP/HTTPS | UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443 |

Content Delivery System

The Content Delivery System (CDS) establishes a connection between the MFD and Canon Universal Gateway (UGW). It provides device firmware and application updates.

Table 5 Content Delivery System Data Overview

| Description | Data Sent | Protocol/Port | Port |
|---------------------------------------|---|---------------|-------------------|
| Communication between the MFD and UGW | Device serial number Firmware version Language Country Information relating to the device EULA | HTTP/HTTPS | TCP/80 TCP/443 |
| Communication between the UGW and MFD | Test file (Binary random data) for communication testing Firmware or MEAP application binary data | HTTP/HTTPS | TCP/80 TCP/443 |

A specific CDS access URL is pre-set in the device configuration.

If there is a requirement to provide centralised device firmware and application management from within the infrastructure, a local installation of iWMC with Device Firmware Upgrade (DFU) plug-in and Device Application Management plug-in will be required.

Remote Support Operator's Kit

The Remote Support Operator's Kit (RSOK) provides remote access to the device control panel. This server-client type system consists of a VNC server running on MFP and Remote Operation Viewer VNC Microsoft Windows client application.

Figure 12 Remote Support Operator's Kit (RSOK) Setup

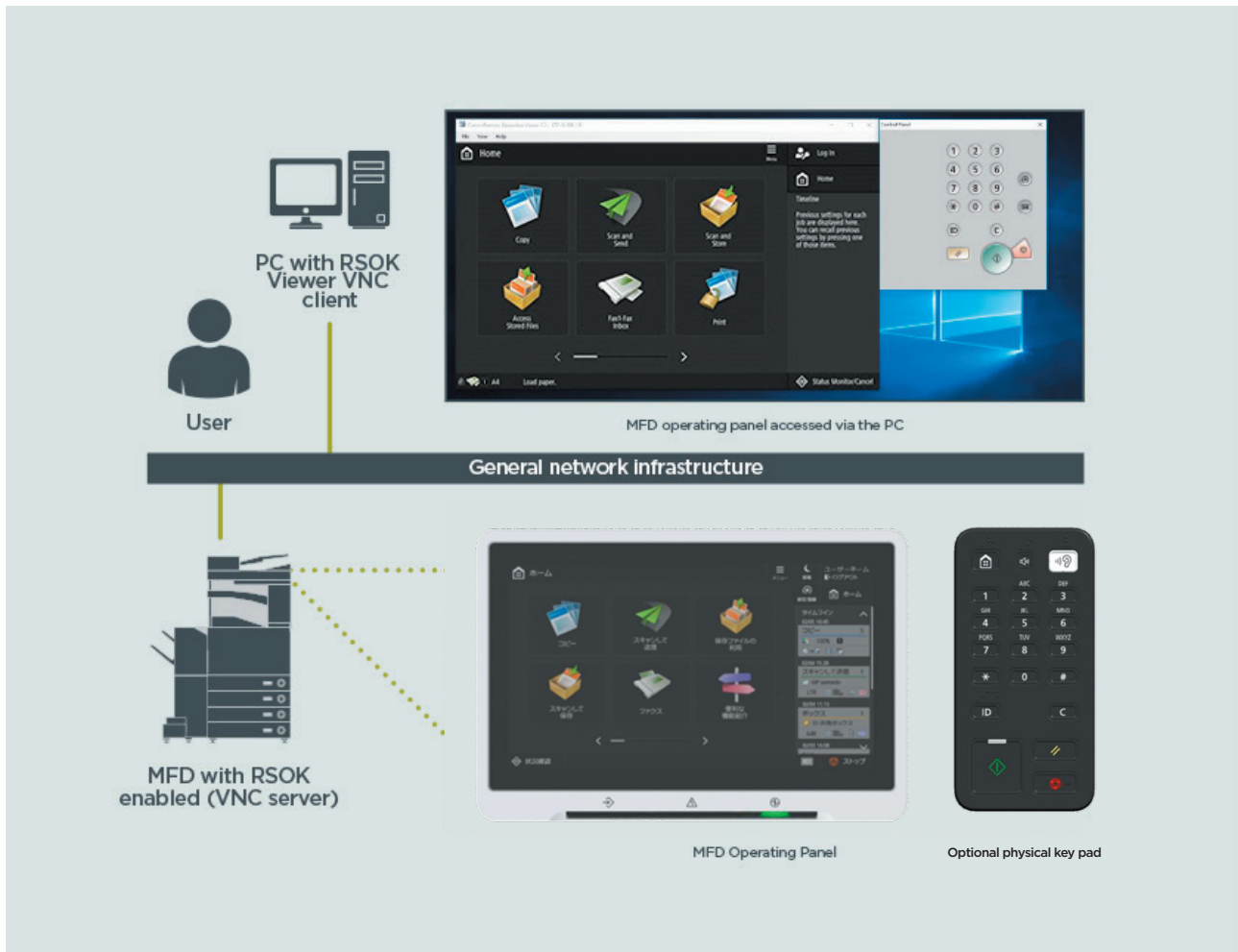


Table 6 Remote Support Operator's Kit Data Overview

| Description | Data Sent | Protocol/Port | Port |
|-----------------------------|---|-----------------------------|------|
| VNC password authentication | User password | DES encryption | 5900 |
| Operation Viewer | Device control panel - screen data - hardware key operation | Version 3.3 RFB protocol | 5900 |

APPENDIX

Canon imageRUNNER ADVANCE Security Related Features

The imageRUNNER ADVANCE platform provides remote configuration through a web services interface known as the Remote User Interface (RUI). This interface provides access to many of the device configuration settings and can be disabled if not permitted and password protected to prevent unauthorised access.

Whilst the majority of the device settings are available through the RUI, it is necessary to use the device control panel to set items which cannot be set using this interface. Our recommendation is to disable any unused services and tighten the controls on those needed. To provide flexibility and support, the Remote Service Operator's Kit (RSOK) provides remote access to the device control panel. This is based on VNC technology consisting of a server (the MFD) and a client (a network PC). A specific Canon client PC viewer is available which provides simulated access the control panel keys where needed.

This section gives an overview of key imageRUNNER ADVANCE security related features and their configuration settings.

Interactive online User Manuals are available from <https://oip.manual.canon/> giving details that not only cover security related features. Start by selecting the appropriate product type (e.g. imageRUNNER ADVANCE DX), click the search icon and enter your search criteria. Below are a few general areas that are worth considering.

Managing the Machine

To reduce leakage of personal information or unauthorised use, constant and effective security measures are required. By designation of an administrator to handle device settings, user management and security settings can be restricted to those authorised only.

Point your web browser to the link below and enter **administrator configuration** in the search box. This will give information related to:

- Basic management of the device
- Limitation of risks by negligence, user error and misuse
- Device management
- Management of System Configuration and Settings

<https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/>

IEEE P2600 Standard

A number of imageRUNNER ADVANCE models are IEEE P2600 compliant which is a global information security standard for multifunctional peripherals and printers.

The link below describes the security requirements defined in the IEEE 2600 standard, and how the device functions meet these requirements.

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

IEEE 802.1X Authentication

When there is a requirement to connect to an 802.1X network, the device must authenticate to ensure that it is an authorised connection.

Point your web browser to the link below and enter **802.1X** in the search box.

<https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/>



Applying a Security Policy to the Machine

The latest imageRUNNER ADVANCE models allow multiple device security settings, the security policy, to be managed in batch via the RUI. A separate password can be used permitting only the security administrator to modify the settings.

Point your web browser to the link below and enter **Applying a Security Policy to the Machine** in the search box. This will give information related to:

- Using a Password to Protect the Security Policy Settings
- Configuring the Security Policy Settings
- Security Policy Setting Items

<https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/>

Managing Users

Customers requiring a higher level of security and efficiency can utilise either built-in functionality or use a print management solution such as uniFLOW.

For further details on our print management solutions, please contact our local representatives or refer to the uniFLOW product brochure.

Configuring the Network Security Settings

Authorized users may incur unanticipated losses from attacks by malicious third parties, such as sniffing, spoofing, and tampering of data as it flows over a network. To protect your important and valuable information from these attacks, the machine supports numerous features to enhance security and privacy.

Point your web browser to the link below and enter **Configuring the Network Security Settings** in the search box. This will give information related to:

The link below details:

- Preventing unauthorised access
- Connecting to a Wireless LAN
- Setting up the network environment

<https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/>

Managing Hard Disk Data/Solid State Drive

The device hard disk drive is used to store the device operating system, configuration settings and job information. Most device models provide full disk encryption (compliant to FIPS 140-2) pairing it to the specific device preventing it from being read by unauthorised users. A preparatory Canon MFP Security Chip is certified as a cryptographic module under the Cryptographic Module Validation Program (CMVP) established by the U.S. and Canada, as well as the Japan Cryptographic Module Validation Program (JCMVP).

Point your web browser to the link below and enter **Managing Hard Disk Data** in the search box.

<https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/>

For information related to Data sanitisation with products using SSD technology point your web browser to the link below and enter **Initialise All Data** in the search box.

<https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/>

SECURITY POLICY SETTINGS OVERVIEW

The third generation of the imageRUNNER ADVANCE models introduce the Security Policy Settings and Security Administration User. This requires successful login of the Administrator and, if configured, an additional Security Administrator login with an additional password.

The table below details the settings available.

| 1. Interface | Notes |
|---|---|
| Wireless Connection Policy | |
| Prohibit Use of Direct Connection | <Use Wi-Fi Direct> is set to <Off> It is not possible to access the machine from mobile devices |
| Prohibit Use of Wireless LAN | <Select Wired/Wireless LAN> is set to <Wired LAN> It is not possible to establish a wireless connection with the machine via a wireless LAN router or access point |
| USB Policy | |
| Prohibit use as USB device | <Use as USB Device> is set to <Off> You will not be able to use the print or scan functions from PCs connected via USB) when use as a USB device is prohibited |
| Prohibit use as USB storage device | <Use USB Storage Device> is set to <Off> It is not possible to use USB storage devices However, the following service functions still work even if "Prohibit use as USB storage device" is ON <ul style="list-style-type: none"> • Firmware update by USB stick (from download mode) • Copying the Sublog data from device to USB (LOG2USB) • Copying the report from device to USB (RPT2USB) |
| Network Communication Operational Policy | |
| Note: These settings do not apply to communication with IEEE 802.1X networks, even if the check box is selected for [Always Verify Server Certificate When Using TLS] | |
| Always verify signatures for SMS/WebDAV server functions | In <SMB Server Settings>, the <Require SMB Signature for Connection> and <Use SMB Authentication> options are set to <On>, and <Use TLS> in <WebDAV Server Settings> is set to <On> When the machine is used as an SMB server or WebDAV server, digital certificate signatures are verified during communication |
| Always verify server certificate when using TLS | <Confirm TLS Certificate for WebDAV TX>, <Confirm TLS Certificate for SMTP TX>, <Confirm TLS Certificate for POP RX>, <Confirm TLS Certificate for Network Access>, and <Confirm TLS Certificate Using MEAP Application> are all set to <On>, and a check mark is added to <CN> In addition, the <Verify Server Certificate> and <Verify CN> options in <SIP Settings> > <TLS Settings> are set to <On> During TLS communication, verification is performed for digital certificates and their common names |
| Prohibit clear text authentication for server functions | <ul style="list-style-type: none"> • <Use FTP Printing> in <FTP Print Settings> is set to <Off> • <Allow TLS (SMTP RX)> in <E-Mail/I-Fax Settings> <Communication Settings> is set to <Always TLS>, <Dedicated Port Authentication Method> in <Network> is set to <Mode 2>, <Use TLS> in <WebDAV Server Settings> is set to <On> When using the machine as a server, functions that use plain text authentication are not available TLS will be used if clear text authentication is prohibited. Moreover, you will not be able to use applications or server functions, such as FTP, that only support clear text authentication May not be possible to access the machine from device management software or driver |
| Prohibit use of SNMPv1 | In <SNMP Settings>, <Use SNMPv1> is set to <Off> You may not be able to retrieve or set the device information from the printer driver or management software if the use of SNMPv1 is prohibited |
| Port Usage Policy | |
| Restrict LPD port | Port number: 515 <LPD Print Settings> is set to <Off> It is not possible to perform LPD printing |
| Restrict RAW port | Port number 9100 <RAW Print Settings> is set to <Off> It is not possible to perform RAW printing |
| Restrict FTP port | Port number 21 In <FTP Print Settings>, <Use FTP Printing> is set to <Off> It is not possible to perform FTP printing |
| Restrict WSD port | Port number 3702, 60000 In <WSD Settings>, the <Use WSD>, <Use WSD Browsing>, and <Use WSD Scan> options are all set to <Off> It is not possible to use WSD functions |

| | |
|--|--|
| Restrict BMLinkS port | Port number 1900 Not used in European Region |
| Restrict IPP port | Port number 631 You will not be able to use Mopria, AirPrint and IPP if the IPP port is restricted |
| Restrict SMB port | Port number: 137, 138, 139, 445 In <SMB Server Settings>, <Use SMB Server> is set to <Off> It is not possible to use the machine as an SMB server |
| Restrict SMTP port | Port number 25 In <E-Mail/I-Fax Settings> > <Communication Settings>, <SMTP RX> is set to <Off> SMTP reception is not possible |
| Restrict dedicated port | Port number: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 You will not be able to use the remote copy, remote fax, remote scan, or remote print functions, or applications, etc if the dedicated port is restricted |
| Restrict Remote Operator's Software port | Port number 5900 <Remote Operation Settings> is set to <Off> It is not possible to use remote operation functions |
| Restrict SIP (IP Fax) port | Port number: 5004, 5005, 5060, 5061, 49152) <Use Intranet> in <Intranet Settings>, <Use NGN> in <NGN Settings>, and <Use VoIP Gateway> in <VoIP Gateway Settings> are all set to <Off> It is not possible to use IP fax |
| Restrict mDNS port | Port number 5353 In <mDNS Settings>, the <Use IPv4 mDNS> and <Use IPv6 mDNS> options are set to <Off> <Use Mopria> is set to <Off> It is not possible to search the network or perform automatic settings using mDNS It is also not possible to print using Mopria™ or AirPrint |
| Restrict SLP port | Port number 427 In <Multicast Discovery Settings>, <Response> is set to <Off> It is not possible to search the network or perform automatic settings using SLP |
| Restrict SNMP port | Port number 161 You may not be able to retrieve or set the device information from the printer driver or management software if the SNMP port is restricted In <SNMP Settings>, the <Use SNMPv1> and <Use SNMPv3> options are set to <Off> |

| 2. Authentication | Notes |
|--|---|
| Authentication Operational Policy | |
| Prohibit guest users | <ul style="list-style-type: none"> <Advanced Space Settings> > <Authentication Management> is set to <On> <Login Screen Display Settings> is set to <Display When Device Operation Starts> <Restrict Job from Remote Device without User Auth> is set to <On> It is not possible for unregistered users to log in to the machine Print jobs sent from a computer are also cancelled |
| Force setting of auto logout | This setting is for logging out from the control panel This does not apply to other methods of logging out (settable range 10 sec – 9 minutes) <Auto Reset Time> is enabled The user is automatically logged out if no operations are performed for a specified period of time Select [Time Until Logout] on the Remote UI setting screen |
| Password Operational Policy | |
| Prohibit caching of password for external servers | This setting does not apply to passwords the user explicitly saves, such as passwords for address books, etc <Prohibit Caching of Authentication Password> is set to <On> Users will always be required to enter a password when accessing an external server |
| Display warning when default password is in use | <Display Warning When Default Password Is in Use> is set to <On> A warning message will be displayed whenever the machine's factory default password is used |
| Prohibit use of default password for remote access | <Allow Use of Default Password for Remote Access> is set to <Off> It is not possible to use the factory default password when accessing the machine from a computer |
| Password Settings Policy (The policy will not apply to department ID management or PIN) | |
| Set minimum number of characters for password | Minimum Number of characters settable between 1 and 32 |
| Set password validity period | Validity Period settable between 1 and 180 days |
| Prohibit use of 3 or more identical consecutive characters | |
| Force use of at least 1 uppercase character | |
| Force use of at least 1 lowercase character | |
| Force use of at least 1 digit | |
| Force use of at least 1 symbol | |
| Lockout Policy | |
| Enable lockout | Does not apply to department ID/mail box PIN, PIN or secure print authentication, etc Lockout Threshold: Settable between 1 - 10 times Lockout Period: Settable between 1 - 60 minutes |

| 3. Key/Certificate | Notes |
|--|--|
| Prohibit use of weak encryption | Applies to IPsec, TLS, Kerberos, S/MIME, SNMPv3, and wireless LAN You may not be able to communicate with devices that only support weak encryption |
| Prohibit use of key/certificate with weak encryption | Applies to IPsec, TLS, and S/MIME If you use a key/certificate with weak encryption for TLS, it will be changed to the pre-installed key/certificate. You will not be able to communicate if you are using a key/certificate with weak encryption for functions other than TLS |
| Use TPM to store password and key | Only available for devices with TPM installed. Always back up the TPM keys when TPM is enabled Refer to the user manual for details Important when TPM settings are enabled: <ul style="list-style-type: none"> • Make sure to change the “Administrator” password from the default value, to prevent a third party other than the administrator from being able to back up the TPM key. If a third party takes the TPM backup key, you will not be able to restore the TPM key • For the purpose of enhanced security, the TPM key can only be backed up once. If the TPM settings are enabled, make sure to back up the TPM key on to a USB memory device, and store it in a secure place to prevent loss or theft • The security functions provided by TPM do not guarantee complete protection of the data and hardware |

| 4. Log | Notes |
|------------------------------|--|
| Force recording of audit log | <ul style="list-style-type: none"> • <Save Operation Log> is set to <On> • <Display Job Log> is set to <On> • <Retrieve Job Log with Management Software> in <Display Job Log> is set to <Allow> • <Save Audit Log> is set to <On> • <Retrieve Network Authentication Log> is set to <On> Audit logs are always recorded when this setting is enabled |
| Force SNMP settings | Enter SNMP server address In <SNTP Settings>, <Use SNTP> is set to <On> Time synchronization via SNTP is required Enter a value for [Server Name] on the Remote UI setting screen |
| Syslog Log reporting | Enable Syslog destination details when using a Syslog server or SIEM <ul style="list-style-type: none"> • <Username and password> • <SMB server name> • <Destination path> • <Perform export time> |

| 5. Job | Notes |
|--|--|
| Printing Policy | |
| Prohibit immediate printing of received jobs | Received jobs will be stored in fax/I-Fax memory if immediate printing of received jobs is prohibited <ul style="list-style-type: none"> • <Handle Files with Forwarding Errors> is set to <Off> • <Use Fax Memory Lock> is set to <On> • <Use I-Fax Memory Lock> is set to <On> • <Memory Lock End Time> is set to <Off> • <Display Print When Storing from Printer Driver> in <Set/Register Confidential Fax Inboxes> is set to <Off> • <Settings for All Mail Boxes> > <Print When Storing from Printer Driver> is set to <Off> • <Box Security Settings> > <Display Print When Storing from Printer Driver> is set to <Off> • <Prohibit Job from Unknown User> is set to <On>, and <Forced Hold> is set to <On> Printing does not occur immediately, even when printing operations are performed |
| Sending/Receiving Policy | |
| Allow sending only to registered addresses | In <Limit New Destination>, the <Fax>, <E-Mail>, <I-Fax>, and <File> options are set to <On> It is only possible to send to destinations that are registered in the Address Book |
| Force confirmation of fax number | Users are required to enter a fax number again for confirmation when sending a fax |
| Prohibit auto forwarding | <Use Forwarding Settings> is set to <Off> It is not possible to automatically forward faxes |

| 6. Storage | Notes |
|---------------------------------|---|
| Force complete deletion of data | <Hard Disk Data Complete Deletion> is set to <On> |

For full imageRUNNER ADVANCE specifications, please refer to the product website found at <https://www.canon.co.uk/business-printers-and-faxes/imagerunner-advance-dx/>



Canon Inc.
canon.com

Canon Europe
canon-europe.com

English Edition
© Canon Europa N.V., 2021

Canon (UK) Ltd

5 The Square
Stockley Park
Uxbridge
UB11 1ET

Tel: 01895 648 000
www.canon.co.uk

Canon Ireland

3006 Lake Drive
Citywest, Saggart
Co. Dublin, Ireland
Telephone No: 01 2052400
Facsimile No. 01 2052525
canon.ie
