CANON SOLUTIONS AMERICA


# WHITE PAPER:

# CANON imageCLASS/ imageRUNNER SECURITY

September 2019

## INTENT OF THIS DOCUMENT:

*Canon recognizes the importance of information security and the challenges that your organization faces. This white paper provides information security facts for Canon imageCLASS/ imageRUNNER devices sold by Canon Solutions America. It provides details on imageCLASS/ imageRUNNER security technology for networked and stand-alone environments, as well as an overview of product technologies related to document and information security.*

*This White Paper is primarily intended for the administrative personnel of a customer charged with responsibility for the configuration and maintenance of imageCLASS/ imageRUNNER devices. The information in this document may be used to more clearly understand the imageCLASS/ imageRUNNER security-related capabilities offered by Canon. The imageCLASS/ imageRUNNER devices offer capabilities that can help facilitate effective management and security of data processed by the device. Ultimately, it is the customer's responsibility to select the method(s) most appropriate for securing their information.*

*Canon does not warrant that use of the information contained within this document will prevent malicious attacks, or prevent misuse of your imageCLASS/ imageRUNNER devices.*

*Security feature support varies in some cases by model; please refer to the available Security Matrix document for model-level detail. The features reviewed in this white paper include both standard and optional solutions for imageCLASS/ imageRUNNER devices. Specifications and availability subject to change without notice.*

*Table of Contents*

# *Section 1 — Introduction*

## Security Market Overview

In today's digital world, risks to networks and devices come in more forms and from more directions than ever before. From identity theft and intellectual property loss to infection by viruses and malware, IT administrators are tasked with adequately protecting information and assets from threats from the outside as well as within.

Nearly every day destructive threats emerge and undiscovered vulnerabilities are exposed, proving that you can never be too secure. IT administrators need a holistic security strategy that can be applied at every level of the organization — from servers, desktops and devices such as printers and MFPs, to the networks that connect them all.

Increased governmental regulations add an additional layer of strict compliance standards that must be met. Legislation such as Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights Privacy Act (FERPA) and Homeland Security Presidential Directive (HSPD)-12 all require that IT administrators ensure the security, privacy, accuracy and reliability of information receives the utmost attention.

## Imaging & Printing Security Overview

Today's printers and multifunction devices share many similarities with general purpose PCs. They contain many of the same components like memory and in many cases CPUs and hard disks; and some even use mainstream operating systems like Windows. Like any other device on the network, sensitive information may be passed through these units and potentially stored on the device. Yet at many companies printers and multifunction devices are not given the same attention concerning information security.

The Canon imageCLASS/ imageRUNNER Security White Paper has been designed to provide detailed information on how imageCLASS/ imageRUNNER devices can address a wide variety of security concerns.

## Key Security Concentration Areas

Canon recognizes the vital need to help prevent data loss, protect against unwanted device use, and mitigate the risk of information being compromised. As a result, all imageCLASS/ imageRUNNER systems include security features to help safeguard information. Canon imageCLASS/ imageRUNNER security capabilities fall into four key areas:

- Device Security
- Information Security
- Network Security
- Security Monitoring / Management Tools

# Security Highlights

**Document Security Features**
- Scan to Myself (uniFLOW)
- Native device Secured Print
- Encrypted PDF
- Digital Signature PDF
- Fax Forwarding

**Data Security**
- No Hard Disk Drive

**Mail Server Security**
- POP Authentication before SMTP
- SMTP Authentication

**Security Management**
- Security Policy Settings

**Device Security**
- Verify System at Startup

**Network Security**
- SMB 3.0 support
- TLS Encryption
- Cipher Algorithm Selection
- TLS Version Selection (select models)
- IP/MAC Address Filtering
- USB Port On/Off
- Destination Restriction
- IPsec
- IEEE802.1x (Wired)

**Authentication**
- uniFLOW/uniFLOW Online (Opt.)
- uniFLOW Online Express
- Department IDs
- Device Level Log-in(eULM)
- LDAP Server (Lotus Domino and Novell eDirectory) Log-in
- Active Directory Log-in
- Control Card Systems (Opt.)
- Authentication-Proximity Card (Opt.)

# *Section 2 — Device Security*

## imageCLASS/ imageRUNNER Controller Security

The imageCLASS/ imageRUNNER series is built upon a platform that provides strong capabilities related to security and productivity. The architecture centers on an operating system powered by an embedded OS. The source version used by imageCLASS/imageRUNNER devices has been hardened by removing all unnecessary drivers and services so that only the ones essential to its operation are included.

The nature of the embedded operation system and the hardening of the operating system reduce the exposure to exploits as compared to a desktop or server version of a Windows operating system. Some of the security related activities include independent testing by security consulting companies of Canon imageCLASS/imageRUNNER devices during various phases of the development process to address potential vulnerabilities prior to production.

## Authentication

Select Canon imageCLASS/imageRUNNER devices include authentication options which administrators can use to ensure that only approved walk-up and network-based users can access the device and its functions, such as print, copy and Scan and Send features. Beyond limiting access to only authorized users, authentication also provides the ability to control usage of color output, and total print counts by department or user.

## Device-Based Authentication

**Department ID Mode***
An embedded feature within imageCLASS/imageRUNNER devices, the Department ID Management mode permits administrators to control device access. If Department ID authentication is enabled, end users are required to enter a password up to seven digits long before they are able to access the device. Up to 300 Department IDs can be configured and each can be configured with device function limitations, such as limiting printing, copying, and faxing, as well as restricting access to color.

> **The settings can be made under Settings / Registration > Management Settings > User Management > Department ID Management***
> **Setting location may vary by device*

**eULM**
eULM is a server-less login application for imageCLASS/ imageRUNNER, which provides an easy and convenient solution for user authentication. Ideal for small to medium size businesses, eULM's simple user authentication includes card log-in (requires an additional option), PIN code, or user name and password, using local or Active Directory (AD), with minimal IT requirements. eULM delivers simplified tracking, allowing organizations to obtain a simple overview of user or device usage activity.

## Card-Based Authentication

**uniFLOW Card Authentication**
When combined with optional uniFLOW, imageCLASS/ imageRUNNER systems are able to securely authenticate users through contactless cards, chip cards, and PIN codes. uniFLOW supports HID Prox, MIFARE, Legic, Hitag, Magnetic and natively using its own reader, as well as others through potential custom integrations. uniFLOW supports 125 kHz and 13.56 MHz card frequencies.

**Control Cards/Card Reader System**
Canon imageCLASS/ imageRUNNER systems offer support for an optional Control Card/Card Reader system for device access and to manage usage. The Control Card/Card Reader system option requires the use of intelligent cards that must be inserted in the system before granting access to functions, which automates the process of

Department ID authentication. The optional Control Card/Card Reader system manages populations of up to 300 departments or users.

## Password-Protected System Settings

As a standard feature, select imageCLASS/ imageRUNNER device setup screens support password protection to restrict device setting changes from the control panel and Remote UI tool. System Administrators can set network information, system configuration, enable, and disable network and printing protocols among many other options. Canon highly recommends setting an administrator password at time of installation since it controls critical device settings.

## Scan and Send Security

On devices that have Scan and Send enabled, information being sent from the device may be considered confidential and sensitive. For these devices, there are additional security features to prevent confidential information from being accessed.

### Address Book Password

Administrative passwords can be set for Address Book Management functions.
By setting a password for an Address Book, the ability to Store, Edit, or Erase individual and group e-mail addresses in the Address Book is restricted. Therefore, only individuals with the correct password for an Address Book will be able to make modifications.

This is not the same functionality when password protecting an Address Book. Administrators who are looking to Import/Export an Address Book, can select to set a password when exporting the File. That password is then required to Import the Address Book. The Address Book Import/Export function is available through the Remote UI utility.

### Destination Restriction Function

imageCLASS/ imageRUNNER models allow system administrators to control where information can be sent using a destination restriction function. Data transmission to a new destination through the Scan and Send and Fax functions can be restricted, prohibiting transmissions to locations other than the destinations registered or permitted by the System Manager.

By restricting sending of faxes, e-mails and files to new destinations, data can only be sent to previously registered destinations. As you can no longer enter or send to new destinations, setting this mode with an Address Book PIN increases security when sending. Sending is only allowed in the following cases when this mode is set:

- If you specify a destination stored in the Address Book
- If you specify a destination obtained via an LDAP server
- If you specify a destination by pressing a one-touch button
- If you recall stored [Favorite Settings] including destinations

If you select [Send to Myself]

## Print Driver Security Features

### Print Job Accounting

A standard feature in Canon's printer drivers, print job accounting requires users to enter an administrator-defined password prior to printing, thereby restricting device access to those who are authorized to print. Printing restrictions can be set using Department ID credentials.

### Custom Driver Configuration Tool

Administrators can create custom driver profiles for users to limit access to print features and specify default settings, thereby protecting the device against unauthorized use, enforcing internal policies and better controlling output costs. Security conscious settings that can be defined and enforced include duplex output, secure print, B&W only on color devices, watermarks and custom print profiles, as well as hiding any desired functions.
**Refer to CDCT supported driver list*

**USB Block**

USB Block allows the System Administrator to help protect the imageCLASS/ imageRUNNER devices against unauthorized access through the built-in USB interface. Access to the device's USB interface for desktop access and the device's host mode for other USB devices can each be permitted or disabled.

**Go to Settings / Registration > Preferences > External Interface > USB Settings***
**Setting location may vary by device*

Select imageCLASS/ imageRUNNER models have the ability to restrict USB usage for memory, but allow USB usage for peripherals such as card readers. Canon's USB feature provides the capability to view and print from the devices only for non-executable files, such as .pdf, .jpg and .tiff. Executable files cannot be performed on the device, which helps protect against viruses and malware.

## Security Measures to Protect Against Malware and Tampering of Firmware/Applications

Since its inception, the imageCLASS/ imageRUNNER series has been designed with security in mind. Security measures to protect against malware/firmware tampering have been implemented that do not allow for installation or execution of programs without a digital signature applied by Canon when updating firmware, executing processes or installing applications. In order to further assist in the prevention of data disclosure due to unknown attacks/springboard attacks, additional security enhancements have been made for the imageCLASS/ imageRUNNER series.

**Verify System at Startup**
Once enabled, the Verify System at Startup function runs a process when the machine starts or when an application (in Application Library) is executed. The process verifies that the system or application has not been tampered. If tampering of one of these areas is detected, it will either prompt for a firmware update or application reinstall. Standard cryptographic technologies (hash, digital signature) are used for verification.

In order to use this function, the administrator should set "Verify System at Startup" to ON (Default: OFF).

To enable Verify System at Startup, steps are listed here:

Menu > Management Settings > Security Settings > Verify System at Startup > <On> - <Yes> to verify setting change > Device will restart after confirmation

**Setting location may vary by device*

When this function is turned ON, warmup time is increased because the verification process is performed when the device is started. However, it does not affect the time to wake up from sleep mode or the restore time for quick startup, because the verification process is performed at device startup.

# *Section 3 — Information Security*

Protecting your organization's confidential information is a mission that Canon takes seriously. From your documents, faxes and e-mails to the underlying data in memory, Canon has built in many controls to help ensure that your information does not become compromised.

## Document Storage

Canon imageCLASS/ imageRUNNER devices do not contain a built-in hard disk drive (HDD), which ensures print job data is only stored in short-term memory and is automatically deleted once the job complete, device power is shut off, or the job times out. This greatly minimizes the risk of critical data loss at the printer.

## Document Security Capabilities

### Watermark

To discourage the unauthorized copying or sending of confidential information, imageCLASS/ imageRUNNER systems support the ability to embed user-defined text within the background of any print job. Users can define custom or preset watermarks to appear in any position on output.

### Encrypted PDF

The Encrypted PDF mode enables users to encrypt, set password and define permissions for PDF files that are sent to an e-mail address or file server for enhanced security. Only users who enter the correct password can open, print, or change the received PDF file.
Encrypted PDF mode can be used only if an e-mail address or file server is specified as the destination. If a fax number, I-fax address, or inbox is specified as the destination, a user cannot send the job as an encrypted PDF file.
Encrypted PDF files can be saved using the 128bit AES algorithms or the 256bit AES algorithms.

### Digital Signature PDF (Device Signature)

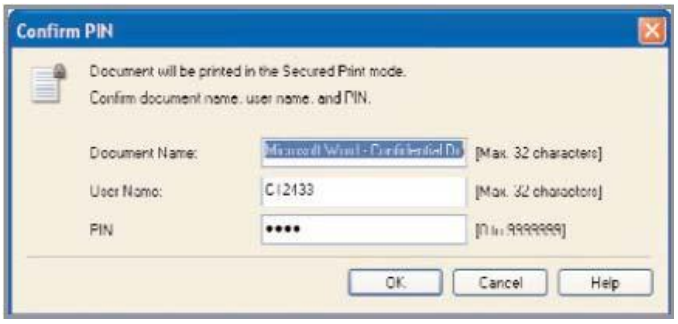
Within Scan and Send, users can add digital signatures that verify the source and authenticity of a PDF document. When recipients open a PDF file that has been saved with a digital signature, they can view the document's properties to review the signature's contents including the name of the device that created the document, the Certificate Authority, system product name, serial number and the Time/Date stamp of when it was created.

The Device Signature PDF use the device signature certificate and key pair inside the machine to add a digital signature to the document, which enables the recipient to verify the device that scanned it.

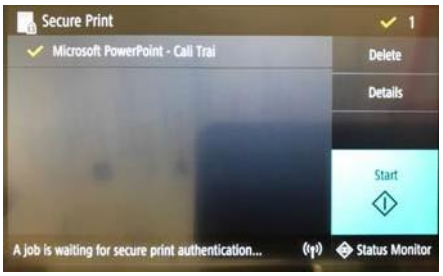
## Secure Printing

### Secured Print*

Secured Print is a print function that holds a job in queue until the user enters the appropriate password at the device. This ensures that the user is in close proximity before the document is printed and minimizes unattended documents left at the device. The imageCLASS/ imageRUNNER device requires the user to set a password in the print driver window when sending a print job from a connected PC. The same password is also required for releasing the job at the device.
Secured print jobs can be set to delete within a specified time frame.
**Select SFP models require additional option for Secured Print.*




Secured Print Screen from the Printer Driver




Secured Print Release Screen at Device UI

**uniFLOW Secure Print**
Exclusive to Canon is uniFLOW, which is optional modular software designed to help reduce costs, improve productivity and enhance security. From a security perspective, uniFLOW contributes to secure printing capabilities by holding jobs at the server until released by the user at any compatible device. From their desktop, users print documents by choosing a single Universal driver. At the chosen device, users can be authenticated using a wide variety of supported methods. Users can then access the uniFLOW client application from the device's control panel and release their job from their queue of pending documents.

## Fax Security - Super G3 Fax Board

Canon imageCLASS/ imageRUNNER MFPs that support fax can be connected to the Public Switched Telephone Network for sending and receiving of fax data. In order to help maintain the security of customer's networks in relation to this potential interface, Canon has designed its Super G3 Fax Boards to function in accordance with the following security considerations:

**Super G3 Fax Board Communication Mechanism**
The modem on the Super G3 Fax Boards does not have Data Modem capability, but only Fax Modem capability. As a result, TCP/IP communication through the phone line is impossible. In addition, there is no functional module such as a Remote Access Service that enables communication between a phone line and a network connection within the device.

**Fax Transmission**
The PC Fax function can fax documents from the PC via Network, using a Fax driver that runs on the PC. However, data transfer from the PC via Network to the device and data transfer (FAX transmission) from the phone line via the G3 FAX board is structurally separated.

**Fax Received**
Although a received fax document can be automatically forwarded to a network, it is not possible to breach the network in either instance as these capabilities are afforded following completion of facsimile communication. Since the data stored is in a format proprietary to Canon, there is no threat of virus infection. Even if the device receives a data file pretending to be a FAX image data but contains a virus, the received data must be decoded first. While trying to decode the virus the phone line will be disconnected with a decode error and the received data will be discarded. The Super G3 Fax Boards cannot receive data files, but are only capable of receiving and decoding facsimile transmissions. As a result, virus-laden files sent to an imageCLASS/imageRUNNER MFP via its phone line connection cannot be processed.

## Other Fax Features

**Allow/Restrict Fax Driver Transmissions**
Device can be configured to allow (default) or restrict sending fax transmissions via a PC Fax driver.

**Go to Settings / Registration > Function Settings > TX Settings> TX Fax Settings > Allow Fax Driver TX***
**Setting location may vary by device*

**Allow/Restrict Sending from History (Job Log)**
The device can be configured to allow (default) or restrict recalling the last three addresses, scan settings, or send settings used, for sending.

**Go to Settings / Registration > Function Settings > TX Settings > Common Settings > Restrict Resending from Log* [ON: Prohibit fax redialing, OFF: Allow fax redialing (Default)]**
*Setting location may vary by device

**Fax Forwarding**
The Fax Forwarding function allows imageCLASS/imageRUNNER MFPs to forward inbound fax transmissions to specific recipients stored in the address book. This is done by setting predetermined conditions or storing faxes in memory for later printing rather than permitting incoming messages to be left in an open output tray.

**Fax Destination Confirmation**
To help prevent faxed documents from being inadvertently sent to the wrong destination, select imageCLASS/ imageRUNNER MFPs offer a Confirm Entered Fax Number feature for additional protection. When enabled on the device by an administrator, users will be prompted to re-enter the recipient's fax number prior to sending in order to confirm that it matches the original one specified. If the fax numbers do not match, the user will be prompted to enter the original number again and re-confirm.

# *Section 4 — Network Security*

**Network and Print Security**

Canon imageCLASS/ imageRUNNER devices include a number of configurable network security features that assist in securing information when network printing is deployed. 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 as desired.

**Enabling/Disabling Protocols/Applications**

Through Canon's device setup and installation utilities, network administrators are provided with the ability to configure the specific device protocols and service ports that are accessible. As a result, unwanted device communication and system access via specific transport protocols can be effectively blocked. Canon imageCLASS/ imageRUNNER devices have the ability to disable unused TCP/IP ports to further secure the devices. Disabling ports may affect the available functions and applications on the device.

Configurable ports include:

| Name | Port | Default | Description | Setting |
|---|---|---|---|---|
| **TCP** | | | | |
| LPD | 515 | ON | LPD print | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [LPD Settings] |
| RAW | 9100 | ON | RAW print | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [RAW Settings] |
| HTTP | 80 | ON | World Wide Web HTTP | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [HTTP Settings] |
| HTTPS | 443 | OFF | HTTP over TLS/SSL | [Settings/Registration: System Management Settings: Security Settings] > [Remote UI Settings] -> [Use TLS] [Settings/Registration: System Management Settings: Network Settings] -> [TCP/IP Settings] -> [Network Link Scan Settings] -> [Use TLS] |
| HTTPS | 10443 | | HTTP over TLS (used for IPPS) | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [IPP Print Settings] -> [Use SSL] |
| POP3 | 110 | OFF | Post Office Protocol 3 | [Settings/Registration] -> [TX Settings] -> [Network Settings E-mail/I-Fax Settings] |
| SMTP | 25 | OFF | Simple Mail Transfer Protocol | [Settings/Registration] -> [TX Settings] -> [Network Settings E-mail/I-Fax Settings] |
| IPP | 631 | ON | Internet Printing Protocol | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [IPP Settings] |
| canon-mfnp | 8610 | ON | Canon MFNP Service | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| canon port | 47545 | ON | Admin Port | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| canon port | 47547 | ON | CPCA-Security port | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| **UDP** | | | | |
| SNMP | 161 | ON | SNMP | [Settings/Registration] -> [Network Settings] -> [SNMP Settings] |
| SLP | 427 | ON | Service Location Protocol | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [Multicast Discovery Settings] |
| WSD | 3702 | ON | WSD WS-Discovery | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [WSD Settings] |
| netbios-ns | 137 | ON | NETBIOS Name Service (SMB) | - |
| netbios-dgm | 138 | ON | NETBIOS Datagram Service (SMB) | - |
| IPsec | 500 | OFF | IPsec IKEv1 | [Security Settings]->[IPSec Settings] |
| mDNS | 5353 | ON | mDNS (AirPrint & Mopria) | [Settings/Registration] -> [Network Settings] -> [TCP/IP Settings] -> [mDNS Settings] |
| canon-mfnp | 8610 | ON | Canon MFNP Service | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| canon port | 9007 | ON | Log Resource | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| canon port | 9013 | ON | Calibration Resource | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| canon port | 47545 | ON | Admin Port | [System Settings] -> [Network Settings] -> [Enable Dedicated Port] |
| uniFLOW | 53216 | ON | uniFLOW Port | - |

*Note: Settings may vary by model. Port usage varies based on device functionality available.*

**IP Address Filtering**

IP Address Filtering is a function to permit or reject reception and/or transmission of packets from specified IP Addresses. Administrators can decide to enable IP Filtering and can specify filtering options (Permit/Reject).

Up to 16 individual IP addresses or IP address ranges can be specified. The default value of all options for this feature is "Disable" (permit reception).

Permission or restriction of an IP address or range will permit or reject access to the following target applications (individual permission/rejection of specific applications is not available):

LPD, RAW, SMB, FTP, HTTP (IPP), PDF, SMTP, WSD, SNMP, HTTP (RUI), SLP

The setup required for filtering involves configuration of the default policy (either Reject or Permit), followed by registration of the IP addresses to be exempt.

If the default policy is to "Permit," then the IP addresses you want to reject must be registered. Conversely, if the default policy is to "Reject," then the IP addresses you want to permit must be registered. The default value for the default policy is to "Permit" for both reception and transmission.

**Media Access Control (MAC) Filtering***
**Not available on Wi-Fi*

MAC address filtering is useful for smaller networks where administrators can manage controls for specific systems, regardless of the subnet to which they happen to be connected. For environments using Dynamic Host Configuration Protocol (DHCP) for IP address assignments, MAC address filtering can avoid issues that are caused when DHCP leases expire and a new IP address is issued to a system. As with IP address filters, MAC address filters can be used to allow or deny access to specific addresses. Up to 32 MAC addresses can be registered and easily added, edited, or deleted through the Remote UI. MAC address filters take a higher priority than the IP address filters; so necessary devices can be allowed or denied, even if the printer's IP address would dictate otherwise. The imageCLASS/ imageRUNNER Series supports MAC address filtering for received packets (RX) and transmitted packets (TX).

**TLS Encryption**

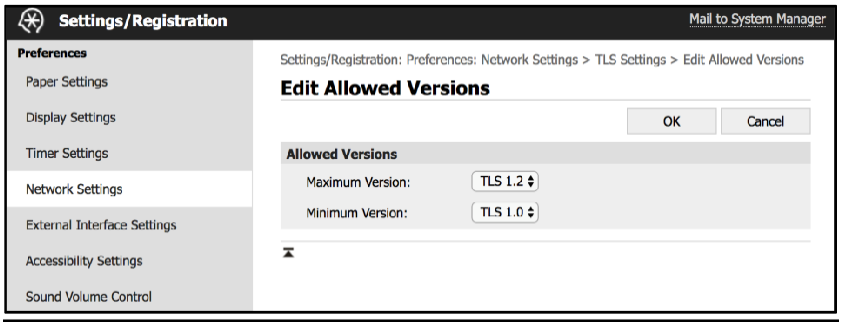
Many organizations are quite diligent about protecting data as it is transferred between PCs and servers or from one PC to another. However, when it comes to transmitting that same data to and from the MFP or printer device, it is almost always sent in clear text. As a result, it may be possible to capture data as it is sent to the printer via the network. Canon helps mitigate this by providing Transport Layer Security (TLS 1.0/1.1/1.2) (for support of some transmissions to and from the imageCLASS/ imageRUNNER device, such as Internet Printing Protocol (IPP), Internet-fax (I-fax) and Remote UI).

The imageCLASS/ imageRUNNER series supports Transport Layer Security, which is a connection-type transport layer protocol for HTTP security. It provides authentication and encryption, as well as detects alterations. Common practice is that a TLS server submits CA certificates with specific expiration dates while a client verifies its authenticity.

## TLS Version Selection

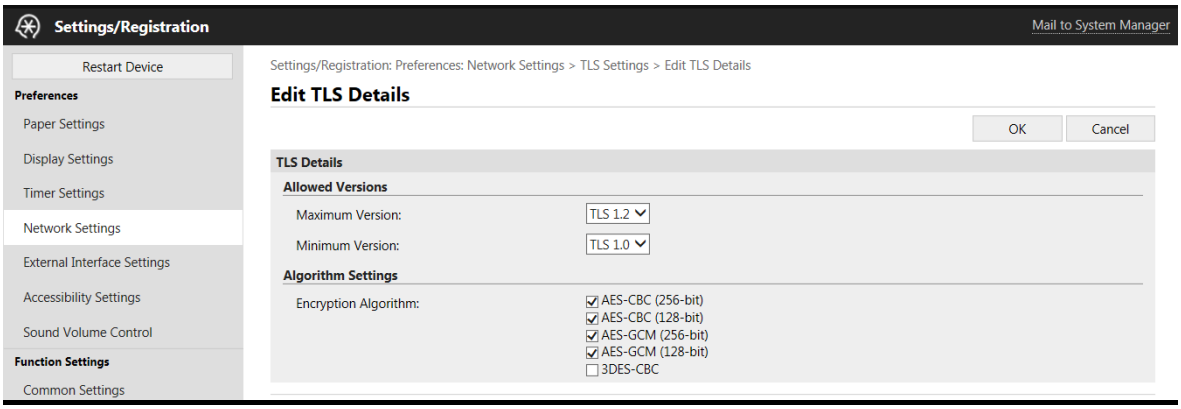
Administrators can specify TLS versions for encrypted communication. Both a maximum version and minimum version can be specified to restrict the available protocol versions. If a vulnerability is discovered in an old version(s) of TLS, the administrator can disable that version in the device to help maintain security.

To modify TLS versions
**Go to Remote User Interface > Settings/Registration > Network Settings > TLS Settings > Allowed Versions***
**Setting location may vary by device*




## Cipher Algorithm Selection (Including disabling 3DES)

The administrator can strengthen security by adapting TLS encryption algorithms to their operation policy. Cypher algorithm selection enables the selection of encryption algorithms/signing algorithms for TLS communication.




## IPv6 Support

IPv6 support, which is available in all imageCLASS/ imageRUNNER devices, provides a more secure network infrastructure, improved traffic routing and easier management for administrators than IPv4.

## IPSec Support

Canon imageCLASS/ imageRUNNER devices support IPSec, which allows users to utilize IPSec (Internet Protocol Security) to help ensure the privacy and security of information sent to and from the device while in transit over unsecured networks.

IPSec is a suite of protocols for securing IP communications. IPSec supports secure exchange of packets at the IP layer, where the packets in the data stream are authenticated and encrypted. It encrypts traffic so that the traffic cannot be read by parties other than those for whom it is intended, it also ensures that the traffic has not been

modified along its path and is from a trusted party, and protects against replay of the secure session. The IPSec functionality of the device only supports transport mode, therefore authentication and encryption is only applied to the data part of the IP packets.

**Authentication and Encryption Method:**
One of the following methods must be set for the device.

- AH (Authentication Header)
  A protocol for certifying authentication by detecting modifications to the communicated data, including the IP header. The communicated data is not encrypted.

- ESP (Encapsulating Security Payload)
  A protocol that provides confidentiality via encryption while certifying the integrity and authentication of only the payload part of communicated data.

**Key Exchange Protocol**
Supports IKEv1 (Internet Key Exchange version 1) for exchanging keys based on ISAKMP (Internet Security Association and Key Management Protocol). IKE includes two phases; in phase 1 the SA used for IKE (IKE SA) is created, and in phase 2 the SA used for IPSec (IPSec SA) is created.

To set authentication with the pre-shared key method, it is necessary to decide upon a pre-shared key in advance, which is a keyword (24 characters or less) used for both devices to send and receive data. Use the control panel of the device to set the same pre-shared key as the destination to perform IPSec communications with, and perform authentication with the pre-shared key method.

To select authentication with the digital signature method, it is necessary to install a key pair file and CA certificate file in advance using the Remote UI, and then register the installed files using the device. Authentication is conducted with the destinations for IPSec communication using the CA certificate.

The types of key pair and CA certificate that can be used for authentication with the digital signature method are indicated below.

- RSA algorithm
- X.509 certificate
- PKCS#12 format key pair

**Wireless LAN**

Many Canon imageCLASS/ imageRUNNER devices support wireless networking. Wireless LAN is IPv6 compliant and supports the latest wireless encryption standards, including WEP, WPA and WPA2.

**IEEE 802.1X**

Canon imageCLASS/ imageRUNNER devices support IEEE 802.1x, which is a standard protocol for port-based Network Access Control. The protocol provides authentication to devices attached to a LAN port and establishes a point-to-point connection only if authentication is successful.

IEEE 802.1X functionality is already supported by many Ethernet switches, and can prevent guest, rogue, or unmanaged systems that cannot perform a successful authentication from connecting to your network.

**SNMP Community String**

Community Strings are like passwords for the management elements of network devices. There is a community string which is used for read-only access to a network element. The default value for this community string for most network devices is often "public". Using this community string an application can retrieve data from the imageCLASS/ imageRUNNER device’s Management Information Base (MIB) elements. There is also a read-write community string, and its default value is usually “private.” Using the read-write community string, an application

can actually change values for MIB variables.

Canon imageCLASS/ imageRUNNER devices use public and private as the default SNMP community strings, but these may be renamed to a user-defined value for increased security. In addition, the systems support SNMPv3, which provides greater security by protecting data against tampering, ensuring access is limited to authorized users through authentication and encrypting data sent over a network.

To modify SNMP community strings go to Settings / Registration > Preferences > Network > SNMP Settings.

**Scan and Send -Virus Concerns for E-mail Reception**

For imageCLASS/ imageRUNNER MFPs with Scan and Send capabilities enabled, when data is received, the email text is separated from any file attachments, and only JPEG/TIFF image files are printed and transferred. The device will discard any attachments of a different file format in e-mail message upon receipt, including attached viruses.

Scan and Send-enabled devices support POP and SMTP as e-mail reception protocols.

## Mail Server Security

When the Scan and Send on imageCLASS/ imageRUNNER MFPs is enabled, the internal mail service is enabled and supports the POP, SMTP APOP, SMTP over TLS, POP over TLS protocols. To protect the service against attack or improper use, administrators can enable additional security features such as SMTP Authentication.

**SMTP Authentication**

To prevent unauthorized users from making use of the device's internal SMTP server, administrators can enable SMTP Authentication and designate a username and password to connect to the server. In addition, administrators can enable TLS for all SMTP send and receive operations.

**POP Authentication Before SMTP**

As an additional layer of security, imageCLASS/ imageRUNNER MFPs support the ability for administrators to enable or disable the POP Authentication before SMTP feature. POP Authentication before SMTP forces a successful login to a POP server prior to being able to send mail via SMTP.

# *Section 5 — Security Monitoring & Management Tools*

Canon provides tools to help organizations enforce their internal company policies and meet regulatory requirements. Whether a single imageCLASS/ imageRUNNER device, or a fleet, is deployed, these solutions provide the ability to audit usage and limit access to features and functions enterprise-wide—at the group and user-level.

**Security Policy Settings**

As document, user, and information security become more important to organizations, administrators need to be sure that the various settings are organized in an accessible location that can be password protected and managed. imageCLASS/ imageRUNNER devices have a common web interface called the Remote User Interface, where administrators are able to do the following:

- Set passwords for access to device settings
- Access and review current security settings
- import and save changes to security settings

**imageWARE Enterprise Management Console**

imageWARE Enterprise Management Console (EMC) is a highly scalable web-based management utility for administrators that delivers a streamlined, centralized point of control for all devices installed across an enterprise. The software makes it easier for organizations to securely manage one or more systems remotely across a network. To aid in implementing and managing a printer and MFP infrastructure, imageWARE Enterprise Management Console facilitates the secure distribution of device configuration information and address books using TLS encryption.

**Device Configuration Management Plug-in**
Allows administrators to configure device and interface settings as required and push the settings out to multiple devices. Provides the ability to back-up or restore detailed device settings to help save significant time and resources for IT departments.

**Device Firmware Update Plug-In**
Allows administrators to push out firmware updates to the fleet.

**Restricting Device Setup Screens**
** Individual device support may vary*

Administrators can lock-out access to device setup screens for unauthorized users from the control panel and Remote UI utility in an effort to protect its configuration information.

# *Section 6 — Conclusion*

Since initially introduced, the highly successful Canon imageCLASS/ imageRUNNER series of printers and MFPs have grown in both the breadth and depth of features and functions. As with any networked device, imaging and printing devices must be included within the broader context of the company's overall security strategy to help ensure the confidentiality, integrity and availability of information.

When properly deployed, the devices can be effectively protected against vulnerabilities from either malicious or unintentional use. Combined with advanced monitoring and management tools for auditing and centralized administration, the systems can meet the demand for increased productivity and strong security.

Canon is committed to helping our customers meet their objectives related to security of their critical information, and is continuing to develop new technologies in this area. For more information, please visit http://www.usa.canon.com.

**Please find model-level detail regarding security support on the available Security Matrix document.**

The information provided in this document is the most current information available at the time of its creation. Canon hereby expressly disclaims all warranties of any kind, express or implied, statutory or non-statutory, in relation to the information provided in this document.

In no event shall Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers be liable for any direct, special, consequential, incidental or indirect damages of any kind (including without limitation loss of profits or data or personal injury), whether or not Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers have been advised of the possibility of such damages, and Canon, Canon's subsidiaries or affiliates, their licensors, distributors or dealers shall not be liable for any claim against you by a third party arising out of the use or performance of canon's products or information referenced herein.

**Regulatory Disclaimer:**
Statements made in this document are the opinions of Canon U.S.A. None of these statements should be construed to customers or Canon USA's dealers 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.

CANON SOLUTIONS AMERICA

csa.canon.com

Canon Solutions America
One Canon Park Melville,
NY 11747

All specifications and availability are subject to change without notice.