



SECURITY TERMS DECODED

Term	Definition
HDD	Hard Disk Drive (HDD); data storage hardware located within the printer.
Encryption	Process of converting printer information or data into a code, specifically generated to help prevent unauthorized access.
SSL Encryption	Security protocol for establishing encrypted links between web servers and printers with online communication.
TLS Encryption	Security protocol that provides privacy and data integrity between two devices or applications. Successor to SSL Encryption.
IPSec	Internet Protocol Security (IPSec); a network protocol suite that authenticates and encrypts the packets of data sent to and from a networked printer or MFP.
SMB 3.0	Protocol that provides a way for applications to read and write to files and request services from server programs and printers.
POP Authentication	Post Office Protocol (POP) is an application-layer Internet standard protocol used by devices and applications to retrieve email from a mail server.
SMTP Authentication	Account verification used by printers identifying themselves to the mail server through which they intend to send email. Mail servers are specific to the environment or service the user is utilizing. Allowing only registered accounts with a service/environment to send and receive emails.
NTLM Protocol	Suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users for networked printers or MFPs.
SIEM	Security Information and Event Management (SIEM); a third-party solution that provides network administration with real-time insights into their network activity. Alerts can be configured to notify administrators of potential issues or threats.
Root of Trust	Set of functions trusted by the operating system to verify validity of code.
IEEE2600 Certification	Industry standard to guide manufacturers or end users of hard-copy devices (such as MFPs or printers) in the installation, configuration, or usage of these devices and systems.



usa.canon.com/iradvsecurity



This document contains basic definitions of commonly used security industry terms in the context of the MFP market. These terms and concepts have many layers so you should perform your own research and conduct your own due diligence concerning the topics described herein. Canon USA does not make any warranties concerning the accuracy or completeness of the opinions, data and other information contained herein and, as such, assumes no liability for any errors, omissions or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data or other information.

Canon and imageRUNNER are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. All other referenced product names and marks are trademarks of their respective owners. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Specifications and availability subject to change without notice. Not responsible for typographical errors.

©2019 Canon U.S.A., Inc. All rights reserved.
0319-SWDCS-PDF-IH