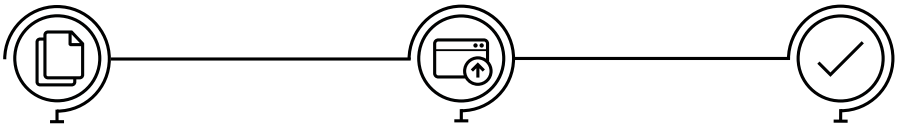
DEVICE HARDENING SERVICE

Canon's Device Hardening Improving the performance of a print device to make it resistant to security related issues. Our service enhances the native security of Canon Devices by applying a secure profile for added protection without the additional effort.



RECCOMMEND **CONFIGURE** **VALIDATE**

BENEFITS FOR YOUR BUSINESS:

- Reduced risk of data loss by protecting data stored in devices throughout their lifetime
- Extend data protection policies to print devices to maintain a secure environment
- Reduce the risk of printer-related security breaches & avoid risk of regulatory fines and damage to brand reputation

POTENTIAL THREATS TO YOUR BUSINESS

- Your devices store and process confidential data, such as financial reports and other sensitive information
- Your devices are connected to the network, which can expose them to potential attacks
- Your devices are often not seen as a security risk, which can make them more of a target

Canon

DEVICE HARDENING SERVICE

DEVICE HARDENING CONFIGURATION

A secure profile configuration that has been fully tested and incorporates recommended cyber security best practices and expectations from buyers of security solutions.

Canon also offers a bespoke service to address customer-specific requirements.

FEATURE	DESCRIPTION
Enable secure data erase option	Data is erased from the device storage automatically, after every job when all pages have been printed/faxed/scanned/copied.
Set Remote User Interface password	Remote User Interface allows access to device settings via web interface. Password allows authorised access to this interface.
Set System Manager password	System Manager allows access to device with administrator privileges. Password is changed from factory default for added protection.
Set Remote Management tool password	Remote Operator's Software Kit allows remote access to device touch panel and controls for service purposes. Password provides extra layer of security.
Enable verification of system integrity at start up	Secure Boot is a native device feature that checks for any tampering of boot code, firmware and MEAP applications at device start up.
Hide device job logs	Block display of job logs generated at the device as these can include file names and usernames.
Disable unused protocols and services	Certain active protocols and ports could increase the risk of attacks so those unused settings are disabled. These include SMB, FTP and IP Fax.
Restrict USB usage	Device cannot be connected to a PC via USB, in order to use print and scan functions. Scanned documents cannot be saved to a USB memory stick.
Restrict connectivity to wireless networks	Device cannot be connected to the corporate network via Wi-Fi.
Prohibit access to guest users	Unregistered users cannot login to use device functions, including releasing print jobs sent via device secure print.
Force auto logout	Users are automatically logged out if no operations are performed for more than 30 seconds.
Restrict use of weak encryption algorithms	Connection to systems supporting weak encryption relating to IPSec, TLS, Kerberos, S/MIME, wireless LAN and SNMPv3 is disabled.

Canon

CONTACT

For more information please contact your local Canon office.

Canon inc.
canon.com

Canon Europe
canon-europe.com

English edition

Canon Europe Ltd
4 Roundwood Avenue
Stockley Park
Uxbridge
UB11 1AF