



Overview of Multi-Function Devices Security Features

Introduction Employees are accustomed to traditional devices such as dedicated printers, photocopiers, scanners and facsimiles that benignly carry out their respective single task. A growing trend in consolidation has resulted in multiple functions being performed by a single unit. The Multi-Function Device (MFD) incorporates scanning, faxing, printing, and copying either directly from the machine itself or from a computer system via a network connection. The embedded computing capabilities of MFDs and network printers, however, create unrecognized risk within the workplace. Organizations need to recognize the potential risks protect the MFDs as they would any other server by implementing security and auditing procedures.



Life Cycle Management should address security in each phase of the life cycle of MFDs and network printers: specification, configuration, installation, use, management and decommissioning.

Working Environments MFDs and network printers are intelligent devices attached to the network. User identification and authentication at both the network and console levels protect devices and the network from unauthorized activity. Physical security such as locks can protect against theft or reconfiguration of the hard drive. Require the wearing of organizational ID badges and challenge unescorted visitors or strangers. When an MFD requires service, technicians should be escorted by knowledgeable employees and use only certified service technicians for repairs.

Basic Security Recommendations

Protection – Protect MFDs and network printers as though they were servers or network devices.

Patches and Updates – Maintain MFDs and network printers: install the latest software updates and security patches.

Connectivity – Restrict network traffic to limit access to those with a need to use the devices. Do not allow external access unless there is an explicit business need.

Password Security – Change all default passwords. Select devices that support passwords instead of simple Personal Information Numbers (PIN).

Change Management – Track every authorized change to the devices and audit periodically to ensure integrity of configuration and software.

Printed Output – Enable the private printing feature so that users must authenticate at the console in order to complete the print job.

Risk	Compensating Policy
Inappropriate use or abuse of resources	Prevent unauthorized access; enforce identification and authentication; log activities; and audit
Installation without appropriate security	Purchase devices with strong security features and certify device configuration before network connection
Lack of control of printed output	Require protection of printed output in security policy