Multifunction Device Hardening Checklist

This checklist contains multifunction device (MFD) hardening requirements. An MFD is sometimes called a multifunction printer (MFP) or all-in-one (AIO) device, and typically incorporates printing, copying, scanning, and faxing capabilities. Because management interfaces for MFDs vary, even within the same product line, this checklist provides general best practices. In order to implement the items on this checklist, consult your MFD's documentation or the vendor. The Information Security Office derived this list from government and industry documents, with a particular focus on configuration issues that are unique to the computing environment at The University of Texas at Austin.

How to use the checklist

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Information Security Office uses this checklist during risk assessments as part of the process to verify that servers are secure.

How to read the checklist

Step - The step number in the procedure. If there is a UT Note for this step, the note # corresponds to the step #.
Check ? - This is for administrators to check off when she/he completes this portion.
To Do - Basic instructions on what to do to harden the respective system
MFD - Reference number in the Defense Information Systems Agency document entitled *Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network*.
UT Note - The UT Note at the bottom of the page provides additional detail about the step for the university computing environment.
Cat I - For systems that include Category-I data, required steps are denoted with the **!** symbol. All steps are recommended.
Cat II/III - For systems that include Category-II or -III data, all steps are recommended, and some are required (denoted by the **!**).
Min Std - This column links to the specific requirement for the university in the Minimum Security Standards for Systems document.

Server Information

MAC Address	
IP Address	
Machine Name	
Asset Tag	
Administrator Name	
Date	

Step	?	To Do	MFD	UT Note	Cat I	Cat II /III	Min Std
		Preparation and Installation					
1		If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.		§	!		5.1
		Network Protocols					
2		Disable all protocols other than IP if they are not being utilized.	01.001	§	!		5.4
3		Assign the MFP a static IP address.	01.002	§	!		
4		Restrict printing/copying/faxing/scanning to the minimum number of subnets practical for the device to function for its group of users.	01.003		!		5.5
5		Use secure communications.		§	!		5.6
		Management Services					
6		Change default passwords and SNMP community strings.	02.001		!	!	5.13
7		Ensure the MFD maintains its configuration state after power-down or reboot. If a full reset is performed, ensure that a process is in place to reconfigure the MFD back to its production state.	02.002		!		
8		Disable unneeded management protocols.	02.003	§	!		5.4
9		Upgrade to patched firmware expediently, in a manner consistent with change control processes.	02.004		!	!	5.2
10		Utilize automated patching notification, if available.		§	!	!	5.3
11		Only allow specific, trusted subnets or hosts to manage the MFD.	02.005		!		5.5
		Print/Copy/Scan/Fax Services					
12		Limit print/copy/fax/scan services to required protocols.	03.001	§	!		5.4
13		If hard disk functionality is enabled, configure the MFD to remove spooled files, images, and other temporary data using a secure overwrite between jobs.	07.001	§	!		
14		Ensure that the MFD provides secure storage for Cat-I data.		§	!		5.7
		Logging					
15		Ensure that logging is enabled on MFDs.	06.001		!		6.1
16		Logs are reviewed on a regular basis.	06.006		!		6.2
17		Logs follow data retention policies.			!		6.3

		Physical Security					
18		Physically secure the MFD in areas with restricted access.		§	!		4.1
19		Lock and prevent access to the hard disk.	08.001	§	!		4.1
20		Ensure that only printer administrators can modify the global configuration from the console by requiring a password.	08.002		!		5.14
21		Ensure that sensitive data is disposed of at device end-of-life.		§	!		5.7

UT Note: Addendum

This list provides specific tasks related to the computing environment at The University of Texas at Austin.

1	If other alternatives are unavailable, this can be accomplished by installing a SOHO router/firewall in between the network and the host to be protected. Performing as much of the configuration as possible while the MFD is not plugged into the network is another alternative.
2	Some printers support non-IP based protocols for compatibility with legacy systems. These might include AppleTalk and IPX/SPX. These protocols are more difficult to monitor and secure, and should be disabled if they are not being used.
3	Giving MFDs static IP addresses or DHCP reservations makes it easier to monitor them and apply access lists on hardware-based firewalls. Consider placing sensitive MFDs on their own VLAN, which may make them easier to identify and secure. It is also strongly advised to give MFDs campus-routed RFC 1918 addresses, so that they are not accessible from the Internet. It is rare that an MFD needs to be accessed from off-campus, and a VPN can be used in those instances.
5	Examples of ways to provide secure communications: • If the MFD supports it, use HTTPS for web-based management rather than HTTP. • If you use SNMP to manage your MFD, and your MFD supports it, choose SNMPv3 for its authentication and encryption features. • Encryption of Category-I data that is output to a printer connected to a network shall be provided through the use of secure printing applications (e.g., JetDirect) or protocols (e.g., IPP over SSL or TLS) to prevent unauthorized network interception. • Rather than printing directly over the Internet, restrict printing to a select group of trusted campus subnets and use the VPN to print over the Internet.
8	Examples of management protocols that can possibly be disabled: • HTTP/HTTPS: Most MFDs include an embedded web server, and HTTP or HTTPS will likely be the primary management protocol for your device. If the MFP does not require remote management, this interface can be disabled. At the very least, see if HTTPS is supported and HTTP can be disabled. • Telnet: Some MFDs provide telnet management interfaces, which are also used by some older management tools. If possible, disable this insecure protocol. • SNMP: If SNMP is not used for device management in your environment, then disable it.
10	MFD upgrades are often manual processes. Patch update notifications might include e-mails from the manufacturer or leasing company.
12	Examples of possible protocols: • Port 9100 (a.k.a. HP JetDirect, socket): Most printing services use this protocol, especially drivers from HP, so you may not be able to disable it. • LPD: LPD is used for printing by many Unix and Linux systems. However, many can now also use CUPS (the Common UNIX Printing System), which allows for printing via a number of protocols. If you do not need LPD, disable it. • IPP: If the Internet Printing Protocol is not used in your environment, then disable it. • FTP: Some printers give you the ability to FTP upload documents to print. This feature is not used in most environments and should be disabled. • SMB: SMB (Windows) printing is often not required, as it is taken care of by other protocols, such as JetDirect. It is also not encrypted. If possible, disable SMB printing. • SMTP: This is often used for scanning and faxing, and can often be disabled.
13	Some MFDs may include the ability to securely erase job-related files in between jobs. Others might require an optional security kit from the manufacturer.
14	Some ways to provide secure storage on MFDs: • User "mailboxes" (which usually contain faxes and scans) must require authentication and authorization. • Some MFDs support encrypted storage, either natively or with the addition of a security kit. If this option is available, consider using it.
18	The level of confidentiality required dictates how MFDs are physically placed. Examples might include: • Kept in a data center with restricted access. • Kept in an office that is attended during business hours and locked after hours. • When a vendor is working on the MFD, the vendor's work is monitored to ensure that security measures are not removed during the course of troubleshooting. If they are removed, they must be put back in place. Refer to the UT Austin Minimum Security Standards for Data Stewardship for more information.
19	If the MFD has a removable hard drive option, then ensure that the drive is locked into the device.
21	For those devices that are not under a specific lease/contract which specifies special handling of the hard drives, follow the university's Hard Drive Destruction Procedures

References

- DISA Sharing Peripherals Across the Network Security Technical Implementation Guide, Version 1, Release 1
- DISA Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network Security Technical Implementation Guide, Version 1, Release 1.2
- HP LaserJet 4345 MFP Security Checklist

- HP Secure Imaging and Printing
- Canon imagerRUNNER Security Kit
- UT Austin Minimum Security Standards for Systems
- UT Austin Minimum Security Standards for Data Stewardship
- UT Austin Data Encryption Guidelines
- UT Austin ISO Consensus Papers
- SANS Institute Gold Paper: Auditing and Securing Multifunction Devices