

SHARP®

THE SHARP SECURITY SUITE

POWERFUL PROTECTION FOR YOUR INFORMATION ASSETS



DATA  SECURITY

THE SHARP SECURITY SUITE

THE LEADER IN DIGITAL INFORMATION SECURITY

Technology makes an ever-increasing contribution to profitability in today's highly competitive business landscape. However, the same technology that enables high productivity in the workplace can easily be compromised if not sufficiently secured. The consequences of inadequate protection could be financial loss, identity theft, risk to intellectual property, or even fines and criminal charges in the most severe cases.

Organizations spend significant capital to protect digital assets from threats, yet frequently overlook one of the most integral devices in use today — the office Multi-Function Peripheral (MFP). The more advanced and integrated MFPs become, the greater the risk to confidential information during the document's life cycle when it is being copied, printed, scanned or faxed. For a comprehensive security strategy to be effective, it is imperative for organizations to demand a greater level of protection from MFP vulnerabilities.

Sharp was the first to address security in digital imaging and received the first Common Criteria Validation for an MFP in 2001. Even today, Sharp remains the highest rated company in validated MFP products and is regarded as one of the industry's greatest security innovators. Businesses and government agencies worldwide have come to depend on this level of assurance, which Sharp pioneered and for which it continues to set the benchmark.



THE RISKS TO OFFICE MULTIFUNCTION PERIPHERALS

An MFP is a powerful asset in your office's environment. Left unsecured however, an MFP can pose one of the greatest threats to your organization. Just consider the types of documents that are copied, printed, faxed or scanned on a daily basis — personal information, financial statements, confidential reports, e-mails, memos, customer data and employee information.

Intellectual property, private and personal information becomes portable once processed by an MFP, and is extremely susceptible to malicious use from both internal and external threats. While not all risks to confidential information are considered malicious, the potential for significant damage from inadequate protection can be only a matter of time.

COMMON VULNERABILITIES

Some of the most common vulnerabilities associated with an unsecured MFP include:

- Loss of productivity
- Regulatory non-compliance
- Loss of access
- Stolen information
- Lawsuits
- Unauthorized use

INTERNAL THREATS

At the device, confidential information can be accidentally or even purposefully copied from stored documents, taken from the output tray or faxed without authorization. Any information stored on a local desktop computer or accessible through the Local Area Network (LAN) can be printed without authorization.

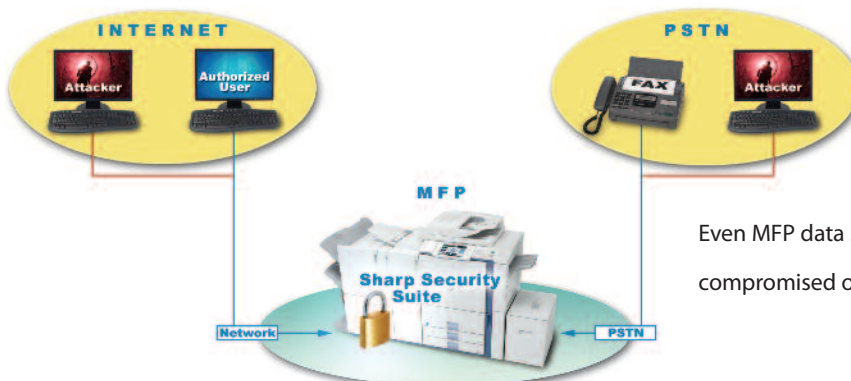


EXTERNAL THREATS

From across a Wide-Area Network (WAN), the Internet or a Virtual Private Network (VPN), information such as stored documents, scan data or print data can be intercepted. In the worst case, a user from the outside can obtain confidential information, unleash a

Denial of Service (DOS) attack, or even place a virus on the device via the network or a phone line. Through a FAX line, or corporate LAN, communications could be intercepted or sent without permission anywhere in the world.

Even MFP data stored on a hard disk drive or in memory could be compromised or even taken off-site and stolen if not protected.



THE SHARP SECURITY SUITE LINE OF DEFENSE

PROTECTING YOUR ASSETS FROM VULNERABILITY

The Sharp Security Suite is effective at preventing unauthorized access to your most confidential information because security has been designed from the ground-up. At the core of the device is a proprietary embedded operating system that is resistant to attack from malicious code and virtually untouchable by viruses, worms or trojan horses. Around this impenetrable core, Sharp MFPs utilize a multi-layered approach to protection — providing better control over the users, devices, ports, protocols and applications that access your Sharp MFPs.

DATA SECURITY

The optional Data Security Kit (DSK) protects and controls the major MFP systems and subsystems (print, copy, scan, fax jobs, network settings, operating system, memory components, local user interface, engine and job controller).

The DSK uses the Advanced Encryption Standard (AES) algorithm on all data before it is written to RAM or Flash memory and the disk. The DSK also provides overwriting routines for deleted data, to ensure that all information is virtually irretrievable by unauthorized users.



ACCESS CONTROL SECURITY

To limit unauthorized access to each device, Sharp MFPs can utilize account codes, user/group profiles, passwords, or external user accounts contained in an LDAP or Active Directory server. All user credentials are transferred using a proven combination of Kerberos, SSL or Digest-MD5 encryption to help avoid interception.



NETWORK SECURITY

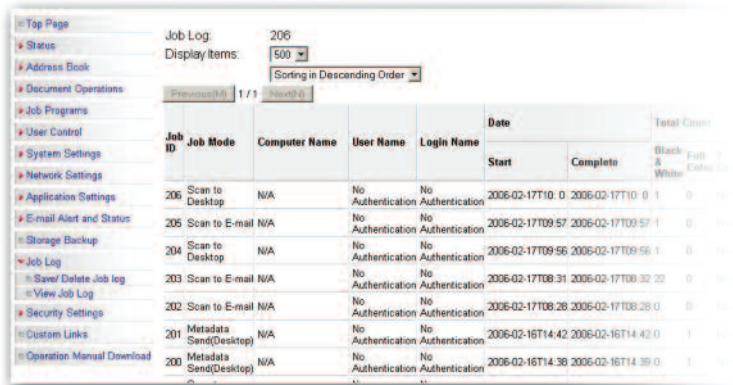
Sharp MFPs feature an intelligent network interface that can limit access to specific computers on a network by IP or MAC address, and selectively enable or disable any protocol or service port on each device. All communications to and from the MFP can utilize Secure Socket Layer (SSL) for secure transmission over the network, and most devices also support SMB, IPv6, IPSec and SNMPv3.

ANTIVIRUS SECURITY

Sharp MFP products use unique embedded firmware and are not based on Windows operating systems. Therefore, Sharp MFP's internal systems are not subject to the same Virus vulnerability as Microsoft operating systems. We believe this approach provides the internal systems of our products with protection against common Windows executable viruses and other similar infectious software programs.



MULTI-LAYERED SECURITY



Job ID	Job Mode	Computer Name	User Name	Login Name	Date	Total Count
206	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T10:00:00	0
205	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T09:57:00	1
204	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T09:56:00	1
203	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:31:00	20
202	Scan to E-mail	N/A	No Authentication	No Authentication	2006-02-17T08:28:00	0
201	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:42:00	1
200	Metadata Send(Desktop)	N/A	No Authentication	No Authentication	2006-02-16T14:38:00	1

FAX SECURITY

The architecture of Sharp MFPs provides a logical separation between the fax telephone line and LAN. It is, therefore, virtually impossible for attackers to gain access to the internal systems of the MFP or the local network.

DOCUMENT SECURITY

Protection for all sensitive documents can be assured through Sharp encrypted PDF files for scanning and printing, or using SSL (Secure Socket Layer) protocols for scanning, printing, e-mail and setup.

AUDIT TRAIL SECURITY

The Sharp MFP internal audit trail, and/or third party application software such as Equitrac Office®, provides comprehensive auditing of all user activity. Certain federal regulations parameters, such as 'to', 'from', 'when' and 'file name' can be logged, reviewed and archived for conformance.

FAX AND NETWORK SECURITY

ACCESS CONTROL SECURITY

AUDIT TRAIL SECURITY

DOCUMENT SECURITY

ANTIVIRUS SECURITY

DATA SECURITY



ROBUST SECURITY SOLUTIONS FOR ANY ORGANIZATION

Sharp MFPs have been rigorously tested and validated to provide the highest level of security protection available today. Sharp remains the first and only company to receive the highest achievable level of Common Criteria Validation for a complete MFP solution — Evaluation Assurance Level 4 (EAL4). While other vendors obtain certification for only individual components of an MFP at the lowest validated level, Sharp is committed to delivering the most comprehensive security solutions possible.

SECURITY FOR THE PUBLIC AND GOVERNMENT SECTORS

With stronger control over all information access and dissemination, the highest level of privacy can be confidently assured for any governmental agency or department. Sharp MFPs have passed the most rigorous evaluations for commercial products available today, and meet the strictest requirements set forth in the National Security Telecommunications, Navy Marine Corps Intranet (NMCI), HSPD-12 (Common Assess Card [CAC]*), Information Systems Security Policy, DISA and (NSTISSP) #11 and DoD Directive 8500.2.

PRIVATE SECTOR REGULATIONS AND PRIVACY

Sharp MFPs provide robust, complete control over information access, transmission and tracking to facilitate compliance with stringent mandates. This will mitigate risk and help avoid any penalties or law suits for non-compliance.

By implementing the Sharp Security Suite, Sharp MFPs can help banks and investment institutions to meet the privacy requirements of the Gramm-Leach-Bliley (GLB) Act. Insurance and health providers can maintain Health Insurance Portability and Accountability Act (HIPAA) compliance with confidence. Businesses across all industries will benefit from the strict controls over financial information required under the Sarbanes-Oxley (SOX) Act.

* With the optional DCL310S Plug-in or MX-EC50 kit (Q4/2009).

SHARP MFP SECURITY LEVELS

HOW SECURE DO YOU NEED TO BE?



Standard Level

Who should use it?

- General office
- SOHO
- Public offices

Benefits

- Confirms user access
- Protects user output
- Adds resistance to attack from malicious codes and viruses

Applications

- Access Control Security (account codes, PIN printing)
- Network Security (IP/Mac Filtering, Port/Protocol Management)

Heightened Level (Includes Standard Level)

Who should use it?

- Enterprise companies
- Human Resources
- Financial
- Accounting
- Healthcare
- Insurance
- Legal
- Education

Benefits

- Virtually eliminates latent document images
- Helps protect stored documents
- Access control authentication
- Helps protect documents in transit
- Audits user activity

Applications

- Data Security Kit (DSK)
- Access Control Security (LDAP and active directory authentication)
- Document Security (document encryption) 128/256 BIT
- Network Security (data and traffic encryption)
- Audit Trail Security (internal and third party log file)

Optimum Level (Includes Heightened Level)

Who should use it?

- Federal agencies, DOD, state offices
- Research & Development

Benefits

- Helps protect from attackers on fax lines
- Provides assurance claims
- Better user access control authentication

Applications

- Common Criteria Validation (CC DSK)
- Fax Security (separation between fax and network lines)
- Network Security (SSL Digital Certificate)
- CAC User Authentication
- Meet IEEE Std. 2600™-2008

SECURITY STANDARDS COMPLIANCE

COMMON CRITERIA-CC AND ISO 15408



Common Criteria
Validated
Sharp Data Security Kit
MX-FRX1, MX-FRX2, MX-FRX3
Ver. M10 Ver. M10 Ver. M10

WHAT IS ISO 15408?

ISO 15408 (International Standard Organization 15408) refers to a set of evaluation standards for security products and systems established by the Common Criteria. This set of criteria is simply referred to as ISO 15408.

THE WORLD'S FIRST AND HIGHEST RATED MFPs

In 2001, Sharp became the world's first MFP manufacturer to achieve Common Criteria Certification for a data security kit and has since maintained the leadership position in the industry. As of March 2009, Sharp can claim no known vulnerabilities in the National Vulnerability Database (NVD) for an MFP. Sharp's commitment to continuous improvement has led to the release of the third-generation of Common Criteria validated MFPs, which have undergone a comprehensive review and achieved a level of EAL3+ and EAL4.

MORE RIGOROUS TESTING MEANS GREATER ASSURANCE

Common Criteria evaluations for commercial security products range from EAL1 to EAL4. While many MFP manufacturers still only achieve EAL2 Validation for their products, Sharp MFPs are measured against a higher level of criteria for more meaningful results in real-world applications. To achieve a level of EAL3 and above, greater disclosure of product information must be provided to the government-controlled testing laboratory.

IEEE STD. 2600™-2008 SECURITY STANDARD

The IEEE 2600 hardcopy security standard, first published in June 2008, is the first industry recognized security standard for MFPs. It specifies security requirements and provides a new International reference to assess the security of the latest generation of MFPs.

Sharp's new line of MFPs (MX-2600N/MX-3100N, MX-4100N/4101N/5001N, DX-C310/C400, DX-C311/DX-C401, MX-C311/C401 and MX-M283/M363/M453/M503) are the first in the industry to meet the new IEEE Std. 2600-2008 security standard requirements.

For more information on how Sharp MFPs help mitigate risk by complying with and exceeding the IEEE-2600-2008 Security Standard requirements, please refer to the IEEE Std. 2600-2008 Hardcopy, Device and System Security document available separately.

For more information on the IEEE Std. 2600 -2800 Security Standard visit www.ieee.org/portal/site.



SHARP NETWORK AND DOCUMENT SECURITY REFERENCE CHART

General	Black and White						Color					
	AR-M237/M277 AR-M257/ M317 Series	AR-M355/ M455 Series	MX-M350/ M450 Series	AR/MX-M550/ M620/M700 Series	MX-M283/M363 M453/M503 Series	MX-M850/ M950/M1100 Series	DX-C310/ DX-C400 DX-C311/ DX-C401 MX-C311/ MX-C401 Series	MX-2300N/ 2700N Series	MX-2600N/ 3100N Series	MX-3501N/ 4501N/MX-3500N Series	MX-4100N/ MX-5001N Series ⁸	MX-5500N/ 6200N/7000N/ 6201/7001 Series
Speed (PPM)	23/27ppm 25/31ppm	35/45ppm	35/45ppm	55/62/70ppm	28/36/45/50ppm	85/95/110ppm	31/40 b/w / 31/40 color ppm	23/27 b/w / 23/27 color ppm	26/31 b/w / 26/31 color ppm	35/45 b/w / 35 color ppm	41/50 b/w / 41/50 color ppm	55/62/70 b/w / 41 color ppm
Functions ¹	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax	Print/Copy/Scan/Fax
Printer Controller	AR-P177/AR-P27	Standard ²	Standard ²	Standard ²	Standard ²	MX-PBX2, MX-PX04	Standard	Standard	Standard	Standard	Standard	Standard
Network Interface Card	AR-P17 ³ , AR-NC5, ³ AR-P27	Standard ²	Standard ²	Standard ²	Standard ²	Standard	Standard	Standard	Standard	Standard	Standard	Standard
Network Scanning Expansion Kit	MX-NSX1	MX-NSX1	MX-NSX1	MX-NSX1	Standard ⁴	MX-NSX1	Standard	Standard	Standard	Standard	Standard	Standard
Facsimile Expansion Kit	AR-FX7	AR-FX12	AR-FX12	AR-FX8	MX-FXX2	MX-FXX1	MX-FXX3	MX-FX1	MX-FXX2	MX-FX2	MX-FXX2	MX-FX3
Hard Disk Drive	—	Standard ⁴	Standard ⁴	Standard	Standard ⁴	Standard	Standard	Standard	Standard	Standard	Standard	Standard
Security Features												
Access Control Security												
Account Codes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Comprehensive Embedded User Access Control	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Authentication	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP	LDAP
Confidential Print	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Follow You Printing™	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}
Card Access Control	Optional ⁷	Optional ⁷	Optional ⁷	Optional ⁷	Optional ^{7, 16}	Optional ⁷	Optional ^{7, 16}	Optional ⁷	Optional ^{7, 16}	Optional ⁷	Optional ^{7, 16}	Optional ⁷
Fax Security												
Confidential FAX	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Seperation Between FAX and Network Connections	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Filter Junk Fax	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Security												
Commercial Data Security Kit	AR-FR12 AR-FR24U, AR-FR25U	AR-FR22U for U Series AR-FR21U for N Series	MX-FRX7U for U Series MX-FRX6U for N Series	AR-FR11U MX-FRX5U	MX-FR15U for U Series MX-FR14U for N Series	MX-FRX8U ⁹	MX-FR12U MX-FR13U MX-FR13U	MX-FRX1U	MX-FR10U	MX-FRX2U	MX-FR11U	MX-FRX3U ⁹ MX-FRX9U ⁹
Common Criteria Data Security Kit	AR-FR12M AR-FR24, AR-FR25	AR-FR22U for U Series AR-FR21U for N Series	MX-FRX7 for U Series MX-FRX6 for N Series	AR-FR11 MX-FRX5	MX-FR15 ¹² for U Series MX-FR14 ¹² for N Series	MX-FRX8 ⁹	MX-FR13 ¹⁰ MX-FR13 ¹⁰	MX-FRX1	MX-FR10	MX-FRX2	MX-FR11	MX-FRX3 ⁹ MX-FRX9 ⁹
EAL Validation Level	EAL3+	EAL3+ for U Series EAL3 for N Series	EAL3+ for U Series EAL3 for N Series	EAL3	EAL3	EAL3	EAL3	EAL3+	EAL3	EAL3+	EAL3	EAL3+
Data Security Kit Features												
Functions ¹	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax	Copy/Print/Scan/Fax
Encrypts Image Data	Fax data only	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹	Yes ¹¹
Hard Disk Overwrite	Not Applicable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RAM Overwrite	Yes	Yes ¹³	Yes ¹³	—	Yes ¹³	—	—	—	—	—	—	—
FAX ROM Overwrite	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to (DOS) Denial of Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to Common Virus Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Control (Anti-Copy)	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Lock User after 3 Retries	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hard Drive Overwrite Features	Not Applicable	—	—	—	—	—	—	—	—	—	—	—
Encryption (# of bit)	—	128	128	128	256	128	256	128	256	128	256	128
# Overwrites	—	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7	Up to 7
Overwrite Method	—	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data	Random Data
Automatic Overwrite after each Job	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automatic Overwrite at Start Up	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manual Overwrite	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Filing												
Protection Method without DSK	—	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection	Folders and/or Document level password protection
Protection Method with DSK	—	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption	Adds encryption
Network Security												
IP Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MAC Address Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password Protected Setup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPSec, IPv6, SSL, TLS	Yes ¹⁴	Yes	Yes	Yes ¹⁴	Yes	Yes	Yes	Yes ¹⁷	Yes	Yes ¹⁷	Yes	Yes ¹⁷
802.1x, IEEE 2600.2008 ¹⁵	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No
SNMPv3	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMB	Yes ¹⁴	No	Yes	Yes ¹⁴	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit Trail Security												
Embedded Log File	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Equitrac Copy Audit Trail	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}	Optional ^{5,6}
Equitrac Print Audit Trail	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵	Optional ⁵
Scan Audit Trail												
Scan to E-mail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Document Security												
Scan Encrypted PDF file	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Print Encrypted PDF file	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 Some Functions Require Optional Equipment
2 Standard on N Series. MX-M350/M450U Series Requires (MX-NBX3) Printer Controller, AR-M355/M455U Series Requires (AR-P21) Printer Controller, MX-M550/M620/M700U Series Requires (MX-NBX1), AR-M550/M620/M700U Series Requires (AR-P19) Printer Controller, MX-M283/M363/M457/M503 requires MX-PB10

3 RJ45 Network Interface Included with the Printer Controller, Certain Operating Systems and Protocols May Require (AR-NC5J) Option
4 Standard on N versions
5 Requires Equitrac Office or Equitrac Express
6 Requires Equitrac Embedded for Sharp's MFPs (for 35ppm and up) or PageControl

7 Common Access Card with DCL310S or 3rd Party Applications with Sharp OSA Technology (for MFPs 35 ppm and up)
8 For MX-5500/6200/7000 Only
9 For MX-6201/7001 Only
10 Available Q4/2009
11 FIPS 197 AES Encryption
12 Available 2010

13 For MFP without Hard Disk
14 For AR-M257/M317 and MX-M550/M620/M700
15. Meet standard requirements
16. Common Access Card with MX-EC50 for N series and MX/DX-C311/C401 (Q4/2009)
17. Only for SSL/TLS



SHARP ELECTRONICS CORPORATION
Sharp Plaza, Mahwah, NJ 07495-1163
1-800-BE-SHARP • www.sharpusa.com

Design and specifications subject to change without notice. Sharp, Sharp OSA® and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. All other trademarks are property of their respective owners.