SHARP®

SECURITY SUITE REFERENCE GUIDE

sharp security
safeguards your business

version 2.4

TABLE OF CONTENTS

INCREASED SECURITY THREATS AND COMPLEXITY

Organizations of all sizes rely on a vast array of technologies to help make daily activities and communication more efficient. Adoption of new platforms such as mobile and cloud, can increase the frequency and complexity of security challenges. The more open and intricate these platforms become, the more corporations and organizations face constant threats that could put sensitive information and business continuity at risk. However, **implementing new technology is essential** to keep up with the speed of business.

Protecting sensitive data is crucial for business continuity.

Threat Types

Insider Security Breach

- Wrongful distribution or viewing of confidential information
- Improper routing of sensitive information
- Unauthorized access to data stored on the MFPs, folders and other services
- Lost laptops and mobile devices

Cyber Attacks

- Email containing malware and bots
- Email Phishing
- DDoS attacks
- Password hacks
- Malware and ransomware attacks through network and system vulnerability

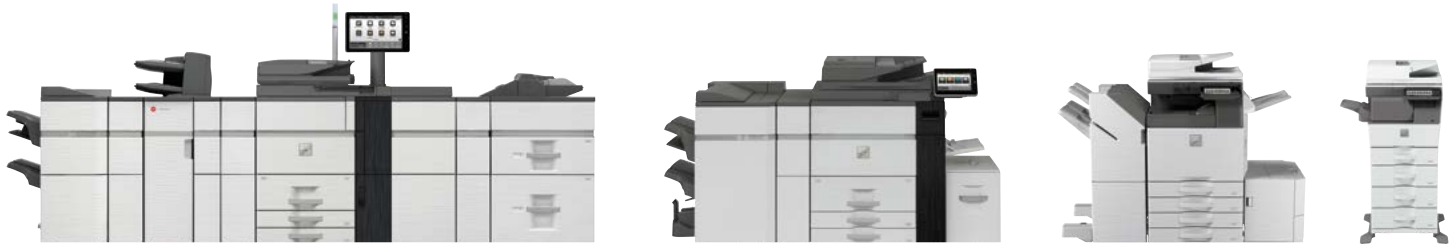
New Risks – Third Platform

Mobile Adoption

- Data and network security vulnerability from BYOD
- Mobile OS vulnerability
- Malicious apps
- Infect mobile devices for monetization
- Misplaced mobile devices

Cloud Services

- Uncontrolled use of cloud services
- Business continuity and vulnerability challenges
- DoS attacks
- Cloud service hijack for ransom



INFORMATION SECURITY IN KEY VERTICAL MARKETS

New technologies such as mobile and cloud services are also transforming numerous vertical markets. However, when organizations adopt new communication platforms, data security and maintaining regulatory compliance become more challenging.

College Campuses, Libraries, Public Organizations

Education – The need for student privacy continues to grow as education records are digitized and shared electronically. Educational institutions must act responsibly, safeguarding students' personal data. Institutions must meet requirements of the Family Educational Rights and Privacy Act (FERPA) as well as the Health Insurance Portability and Accountability Act (HIPAA) on digitalized student information.

Critical Information: • Student Records • Social Security Numbers • Health Information

Defense Contractors, Government Agencies, Department of Defense, Local Governments

Local Government – Local government agencies maintain various types of data including social security numbers, credit card numbers, driver's license numbers, Federal Tax Information (FTI) and more. As the e-Government movement progresses, local government offices are under great pressure to protect sensitive information from hackers. Cybersecurity is one of the most critical components of IT for government agencies. Local government organizations, department entities, and courts, have strict data security mandates as outlined in several security standards, specifications and directives. Among the most stringent and applicable standards for MFPs and printers is ISO 15408/Common Criteria (CC) directed by National Information Assurance Partnership (NIAP).

Critical Information: • Social Security Numbers • Resident Information • Driver's License • Local Government Documents • Police Reports • Contracts

Lawyers, Law Offices, Service Organizations

Legal Services – Lawyers and law firms need to protect their client's data and information. In reaction to the rate of cloud and mobile adoption as well as the growing trend in data conversion requirements for e-discovery, companies offering legal services are forced to meet new regulations and compliances such as the EU General Data Protection Regulation (GDPR) and U.S. Personally Identifiable Information (PII). Proper data classification ensuring only authorized users access to the confidential data will be critical to minimize the impact on legal practices.

Critical Information: • Social Security Numbers • Contracts • Case Information • Client Information

Hospitals, Pharmacies, Healthcare Facilities

Healthcare – The Health Information Technology for Economic and Clinical Health Act (HITECH) and Meaningful Use execution enabled rapid adoption of Electronic Health Record (EHR) systems. The U.S. Department of Health and Human Service (HHS) recognized that advances in electronic technology and digitalized patient records could further risk the privacy and security of confidential health information. The privacy and security protections for individually identifiable health information are strengthened under the rule and national standards of the Health Insurance Portability and Accountability Act (HIPAA). Doctors, hospitals, insurance companies, nursing facilities and other care providers must follow HIPAA to protect patient information, health histories, medication records, billing and insurance information and other electronic healthcare transactions.

Critical Information: • Private Patient Records • Health Histories • Medication Records • Social Security Numbers

Private Companies, Financial Institutions

Financial/Corporate – Financial institutions and business organizations are constantly under threat of information leakage by internal and external sources. All organizations, regardless of size, that are “significantly engaged” in providing financial products or services, such as banks, mortgage lenders, brokerage houses and investment organizations, are guided by the Gramm-Leach-Bliley (GLB) Act to protect confidential records, transactions and customer information. In addition, all public companies need to comply with the Sarbanes-Oxley Acts (SOX). SOX mandates that organizations must store and track business information including electronic communications as well as hard copy documents. In addition, due to increased adoption of online transactions, corporations are required to meet new regulations such as GDPR. IT administrators are challenged to securely and cost-effectively store and manage all corporate and customer information.

Critical Information: • Customer Information • Employee Records • Bank Account Information • Corporate Accounting and Financial Records • Tax Documents • Credit Card Information • Social Security Numbers

PRINTER AND MFP SECURITY

Organizations are under constant threats from malicious attempts to steal and/or modify business data, or gain unauthorized access to their networks. Security threats as well as regulatory compliance requirements can be extended to the printers and multifunction printers (MFPs) that are commonly used in any organization.

Physical Security Threats

Typically, MFPs are located in common areas accessible by multiple people. Unauthorized personnel can potentially access and enter corporate networks when devices are not fully protected. In addition, any information stored on a local desktop computer or a server accessible through the network can be printed without authorization. Meanwhile, at the MFP device, confidential information can be accidentally or even purposely copied from stored documents, taken from the output tray or faxed without authorization.

Network Security Threats

Unsecured access to your company's stored data makes you vulnerable to having it stolen or altered. Furthermore, cyber criminals may obtain confidential information by unleashing a Denial-of-Service (DoS) attack, a phishing attack, or a virus via the network to launch an advanced cyberattack. Phone line communications or network data could easily be intercepted when proper security measures are not implemented. Even MFP data stored on a hard disk drive or in memory could be compromised or stolen if not protected.

Protecting sensitive data is crucial and the end goal.

Today's intelligent MFPs and printers have evolved to include advanced network communications and data storage capabilities. Failing to protect them may result in devastating damage to a company. Potential business impact includes:

- Loss of productivity
- Fines due to regulatory non-compliance
- Loss of access to data and network
- Loss of competitiveness due to stolen information
- Lawsuits

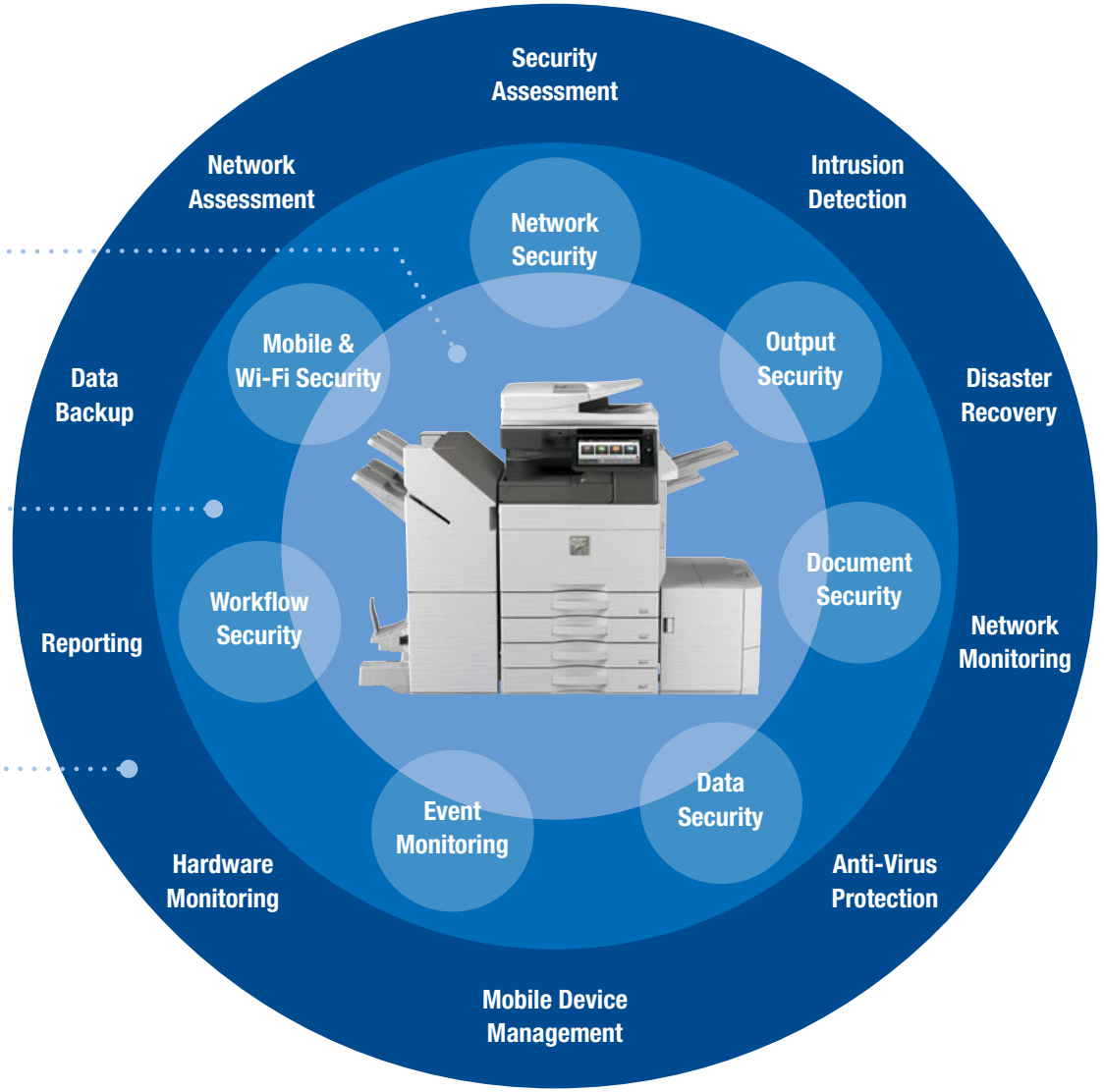
SHARP SECURITY SUITE

Sharp provides a multi-layered approach to help safeguard organizations against security threats. Sharp MFPs and printers are designed to help IT administrators and security officials plan, choose and implement proper risk prevention and control through the comprehensive Sharp Security Suite.

Standard MFP Security & Data Security Kit (DSK)*

Security Management Software

Third Party & IT Service Applications



sharp security
safeguards your business

* Data Security Kit option available on most models.

Security Features That Provide Comprehensive Protection

Sharp MFPs are armed with many advanced security features to help businesses safeguard their data and protect against unauthorized network intrusions and malware attacks. Businesses can achieve optimal protection by following good IT practices and utilizing these features.

Achieve Optimal Security: Check Your MFP's Security Configuration!*

- ✓ Implement secure user access control (Active Directory® or LDAP user authentication).
- ✓ Limit users who have administrator's rights.
- ✓ Apply more complex administrator password rules.
- ✓ Close unused ports and disable unneeded network services and protocols.
- ✓ Use IP and MAC address filtering to limit MFP access to only necessary PCs.
- ✓ Install a Data Security Kit (DSK) or configure built-in data security.
- ✓ Enable the TLS protocol to secure all communications.
- ✓ Ensure that users are assigned to properly configured Authority Groups.
- ✓ Disable unused device functions.
- ✓ Periodically check job and audit logs for suspicious activity.
- ✓ Enable POP3 and SMTP authentication if possible.
- ✓ Change the MFP's SNMP community name from its default "public."
- ✓ Do not "publish" an MFP's IP address outside your organization's firewall.
- ✓ Ensure Wi-Fi and mobile security are properly configured.

* Some features may not be available on all models.

Data Security in Transit or at Rest

Hassle-free erase/overwrite of data and settings completed securely.

Data security is a fundamental component for MFP and printer security. Sharp MFPs and printers include standard and/or optional security features that protect data stored on the device or in transit.

- **Data Encryption**

  When data encryption is enabled on select Sharp MFPs, Advanced Encryption Standard (AES) algorithm 256-bit method is used in communication and on the data before it is written to RAM and the hard disk drive.

- **Data Overwrite**

  Up to 10 times programmable overwrite is used to maximize the data erase efficiency. The data is overwritten by random numbers. In addition, the data overwrite method can be customized to meet each organization's security requirements or it can be set as it is specified in DoD 5220.22-M.

Data Security Kit (DSK) and Common Criteria Certification/ISO-15408

Organizations may require enhanced security features to meet regulatory requirements or mitigate specific threats. The optional Sharp Data Security Kit available on most models brings device security to a higher level with features such as manual data overwrite and auto data overwrite at power-up, hidden pattern printing and detection, and more. In addition, select DSK models are equipped with a Trusted Platform Module (TPM) chip which helps further prevent unwanted access to data storage areas including hard disk drive and solid-state drive.

- **Trusted Platform Module**

  Trusted Platform Module is an industry standard computer chip that uses **cryptoprocessor technology** to protect hardware such as hard disk drives and **solid-state drives** inside MFPs and printers. When a new Sharp MFP is installed with a data security kit, the TPM chip inside the machine initiates a cryptographic key that cannot be accessed by software. A matching cryptographic key is encoded during the boot-up process. If the two keys do not match, access to the device is denied. TPM is an important component of a customer's network strategy and can help protect them from data storage attacks.

The Common Criteria (CC) is a set of guidelines used to evaluate information technology equipment. It is the technical basis for an international agreement and the specification is tested by independent laboratories. Sharp has always aimed to achieve a secure and productive office environment through the development of our digital MFPs. Meeting evolving security standards, such as Common Criteria, is important to ensure organizations confidently handle the most sensitive data on Sharp devices. Recently Sharp achieved the industry's first Common Criteria certification against the latest **Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)**.

- **Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)**

  HCD-PP v1.0 (dated September 10, 2015) is the latest requirement for multifunction printers based on the security requirements specified by the U.S. and Japanese governments, providing the most up-to-date security validation for businesses, government and military offices. It aims to protect the information processed by an MFP from security threats and includes specifications for encryption and firewalls. The HCD-PP v1.0 was developed through the industry collaboration with the National Information Assurance Partnership (NIAP) and the Information-technology Promotion Agency, Japan (IPA). HCD-PP v1.0 now defines security for the MFP as a whole, and as such, reference to the Evaluation Assurance Level ("EAL") is no longer used.

Data and Information Security*

Sharp standard MFP security features coupled with the optional Data Security Kit protect and control the major MFP systems and subsystems (print, copy, scan, fax jobs, network settings, memory components and local user interface). The Sharp data encryption method uses the Advanced Encryption Standard (AES) algorithm 256-bit on all data before it is written to RAM and the hard disk drive. It also can provide up to 10 times data overwriting routines to minimize information leakage. Select Sharp MFPs support DoD 5220.22-M data overwrite for optimal data security.

SHARP STANDARD FEATURES		WITH OPTIONAL DATA SECURITY KIT (DSK)	
Level 1 **Standard Security Features**	**Level 2** **Advanced Security Mode**	**Level 3** **DSK Standard Security Mode**	**Level 4** **HDC Protection Mode**
Basic security including user authentication, network protection, logs, etc.	Basic security plus data overwrite and encryption.	Trusted Platform (TPM) based advanced security including manual data overwrite, firmware digital signature, optional feature restrictions.	Trusted Platform (TPM) based advanced security configured to comply HCD protection profile v1.0 enforcing security and forced feature restrictions.
<Additional Security Layer> Sharp Partner Program Member products and applications.	**<Additional Security Layer>** Sharp Partner Program Member products and applications.	**<Additional Security Layer>** Sharp Partner Program Member products and applications.	**<Additional Security Layer>** No ID card readers, Sharp OSA applications are allowed.

Access Control Security

To limit unwanted access to each device, Sharp MFPs can utilize account codes, user/group profiles, passwords, or external user accounts contained in the local device address book or global user directory. All user credentials are transferred using a proven combination of Kerberos, Transport Layer Security (TLS) or AES 256-bit encryption to help avoid interception. In addition, select Sharp MFPs can be registered as a computer with the Microsoft Active Directory® domain, providing strong Kerberos token-based authentication and authorization. IT administrators can securely and conveniently manage devices and access to “scan-to folders” and “scan-to emails” with an advanced level of control.

* Encryption level and security features vary per model. Please see the Security Compatibility Charts for more details.

Data Security at End-of-Lease

When the device is retired, it is important that the data retained within the device be removed or rendered in an unreadable format. Select Sharp document systems offer standard End-of-Lease features to ensure that all confidential data is overwritten before the device leaves the facility.

- **How is the data erased?**

  When the End-of-Lease feature is executed the data is overwritten up to 10 times. If a DSK is installed or standard MFP security feature is enabled, the data is overwritten with random numbers. The amount of times the data overwrite occurs and custom overwrite methods can be configured.

- **What happens at the completion of End-of-Lease data erase?**

  While data is being erased, the data deletion progress will be displayed. After erasing is completed, the MFP will be rebooted automatically. The data erase completion report will then be printed out.

The following data will be erased using End-of-Lease data overwrite feature:

Sharp helps protect your data and personal information from the first day of operation to the time of trade-in.

Setting Values	Job Image	User Input Data		System Data
• System Settings/Web Settings • Admin Password • Network Settings • Soft Switch	• Job (image) Data on Each Mode • Unprinted Fax/Internet Fax/Direct SMTP Data • Document Filing Data • Data Stored in NAS Area • Image Data in Memory Box • Print Release Job Data	• Address Book • User Information (including User Index/User Count) • Job Program • Organization/Group List/Page Limit Group List/ Authority Group List/ Favorite Operation Group List • Billing Codes • Words Registered in Software Keyboard • Scanner Default Sender • Scanner Default Destination • Fax/I-Fax Forwarding Destination/ Sender/ Allow/Reject Sender	• Polling Protection Number • Dial-in Number • Auto Forward Table • Destination for Document Admin • Fixed Phrase (Text/Image Printing/ Subject/File Name/Body Text/Email Footer/Tracking Information) • Metadata Set • Custom Links • Sharp OSA Embedded Application • Custom Stamp/Custom Watermark • Color Profile • Download Font	• Job Status Completion Queue Data • Job Log • Encrypted Communication Control Information • Keyboard Input Character Translation Information

Data Security During Operation

Organizations are under constant threat of increasingly menacing cyberattacks. To help prevent or better respond to such threats, select Sharp multifunction printers are armed with leading-edge, multi-layered security features, including **Firmware Attack Prevention and Self Recovery**, which can help identify a malicious intrusion and restore the machine firmware to its original state. The **Application Whitelisting** feature detects access attempts to the machine file system and denies access if the source data is not on the whitelist.

Manage your devices, control access, and protect your data.

Additionally, built-in **Authority Groups** help manage and restrict copying, printing and scanning features to safeguard data as well as control costs. Administrators can also apply **Active Directory® Group Policy** to the device on most models, which offers centralized configuration and control for select security and print driver settings. **Sharp Remote Device Manager** (SRDM) enables both IT administrators and service providers to monitor and centrally manage their MFP fleets by maintaining security policies, deploying scheduled admin password changes and more. Sharp MFPs can also help keep confidential documents secure with **Confidential Printing**, which requires users to enter a PIN code to print them. Also, **256-bit data encryption** combined with **up to 10-times data overwrite** helps ensure the customer's information is protected. When it is time to trade the machine in, most Sharp MFPs include an **End-of-Lease** feature that can erase all data and personal information, as well as print a confirmation report for verification.

Critical features that help organizations prevent threats.

- **Firmware Attack Prevention & Self Recovery**

The Firmware Attack Prevention and Self Recovery feature on select Sharp MFPs **helps protect the main unit firmware system files from malicious attacks**. The machine stores a backup copy of the main unit firmware in a hidden partition of the MFP hard disk drive. Each time the MFP is turned on, or wakes from auto-off mode, the main unit firmware running in the machine is compared to the backup copy stored on the hard disk drive using a hash value. If the two hash values do not match, the machine will be halted and display a message prompting the user to turn off the power and turn it back on. This action triggers the machine to restore the main unit firmware running in the machine with the backup copy stored on the hard disk drive. This event is recorded in the machine real-time event log and can also be sent to the administrator via email, as well as included in the customer's syslog or SIEM (system information and event management) system. This feature is standard on select Sharp MFPs and can be enabled through the MFP web user interface System Settings.

Note, if a data security kit is installed on the machine, a higher level of protection is available with the Trusted Platform Module, which supersedes the Firmware Attack Prevention and Self Recovery feature.

- **Application Whitelisting**

Combating IT threats is more challenging when devices are network-connected to offer advanced features. In order to mitigate risks, the Sharp Application Whitelisting feature, available on select Sharp MFPs, protects against unofficial software and application updates by detecting access attempts to the MFP's file system and denying access if the source data is not on the whitelist.

- IT administrators can be notified of whitelisting events via email or integrated with the organization's Syslog or SIEM (Security Information and Event Management) systems using the MFP's audit log feature.

Protect against unauthorized access to the MFP file system with Application Whitelisting.

User Authentication, Authorization and Restriction

Most Sharp MFPs can limit unwanted access with user authentication. All user credentials are transferred using a combination of Kerberos and Transport Layer Security (TLS) to help avoid interception. In addition, select models can be registered with Active Directory® domain offering Kerberos token-based Active Directory authentication. "Secure mode" to request a user password upon logon is also supported for ID card authentication, minimizing the risk of passwords being compromised.

User authentication types:

- Local user list
- LDAP
- Active Directory
- External authority with Sharp OSA®-enabled applications

User authentication methods:

- PIN number
- Username and password
- ID card

Once the user is authenticated, access to certain features are either granted or restricted. IT administrators can securely and conveniently manage devices and access to specific features with an advanced level of control.

Sharp Security Suite helps mitigate threats through authentication and restriction.

Key features for authorization and access restriction:

- Password protected admin access
- Print, scan, copy and fax function control
- Access control for the MFP's HDD
- Page limit control
- Color printing restriction
- Forced pull printing
- Destination entry restriction
- Domain restriction
- Forced scan to logged-in users' email address
- Forced scan to logged-in users' home folder
- Security control and default setting using Active Directory Group Policy with Sharp ADM template files (Device settings and Print Driver settings)

Single Sign-on (SSO) to Network and Cloud Resources

IT administrators often face challenges sustaining productivity while maintaining security. Select Sharp MFPs offer options for single sign-on to add operational convenience while validating user access to the device and network.

When an MFP joins a domain, the MFP establishes trusted relationships with network resources. IT administrators can provide secure Kerberos token-based SSO to network and home folders as well as Microsoft® exchange server.

For Google Drive™ online storage service, Gmail™ webmail service and select cloud services, an OAuth token is used to establish SSO. Sharp provides IT administrators greater flexibility and options to provide convenience to users while maintaining organization's data and information security.

Single sign-on supported resources:

- Network folders and home folders
- Exchange server
- Gmail webmail service
- Cloud services (such as Box™, Google Drive™, OneDrive® for Business and SharePoint® Online)
- Sharp OSA® applications

Network Security

Network security is fundamental in protecting organizations' network and resources from improper use, intrusions, denial-of-service (DoS) attacks and unauthorized access and modification. Sharp MFPs help IT administrators and security officers design comprehensive security environments to ensure only authorized parties and protocols are allowed to access their network with Sharp MFPs and printers.

- Network communication protection via TLS
- SHA-2 certificate
- Wireless LAN communication protection
- Secure protocols such as Kerberos, IPv6, and SMBv3
- IP address and MAC address filtering
- Port management
- Disable/enable features and functions
- SNMPv3 communication
- Device certificates
- CA Certificates
- IEEE802.1X™ authentication

Document Security

Protection for sensitive documents can be achieved through various document security features including encrypted Adobe® PDF files for scanning and printing, and document filing features, which allow files to be retained until they are needed – preventing unauthorized access to confidential information. Secure access to documents for printing and scanning can also be achieved with Synappx Go on your mobile device. This powerful application helps your content move with you throughout the workplace. To learn more about Synappx, please visit the Sharp USA website.

Document security at the device:

- Encrypted PDF
- Secure document filing features
- Pull printing/PIN printing
- Secure watermarks

Document security with Synappx Go:

- Secure print release
- Printing from cloud storage
- Scanning to self or the cloud
- NFC tag for optimized security

Email Security

Email is the most frequently used and critical business communication method at many organizations. Sharp MFPs offer various email security features to enhance data privacy capability to cultivate trust and reputation. For more integrated email security, select Sharp MFPs offer the Email Connect feature which establishes a direct connection for Exchange servers or Gmail. This also ensures the email is sent by the logged in user (not via the generic MFP address). The email containing the scanned document is then stored in user's sent folder. For the Exchange server, all server rules and security (e.g. size limit, destination restrictions) are automatically applied to scan-to-email maintaining the organization's email policy.

- Digital Signature and encryption with S/MIME
- Exchange server integration (authentication and restriction)
- Gmail webmail integration
- Send email from logged in user
- Store sent email on sent item folder
- Domain control
- Destination restriction

Enabling the mobile workforce safely and securely for on-the-go access.

Mobile and Wireless Security

Adoption of mobile technology is critical for organizations to be innovative and agile. However, IT administrators often face risks by allowing personal devices to access critical business information. Sharp provides optimal security for mobile users to connect with the corporate network via the MFPs and printers.

- User authentication (Active Directory, LDAP, Local User List, PIN number)
- SNMP security
- Print retention
- Serverless Print Release (select MFP models)

In addition, select Sharp MFPs support “Access Point” mode which allows mobile users to connect via Wi-Fi for printing from and scanning to their mobile devices – without having to connect through the corporate network. The Access Point mode prevents data exchange between Wi-Fi and wired interfaces.

Audit Trail

Tracking user activities and events are important and helpful to maintain proper security measures. Granular audit log and job log features from Sharp provide comprehensive auditing of all user activities and device events.

- **Job Log**

  Certain regulations require parameters, such as “to,” “from,” “when” and “file name” to be logged, reviewed and archived for conformance.

- **Event Log (Supports RFC 5424/3164 Standard Syslog Protocol)**

  With select Sharp MFPs, the IT team can monitor events such as when/what setting changes were made, which IP address have accessed the device, and when firmware is updated. The MFP’s real-time event log can be integrated with the organization’s syslog or SIEM (Security Information and Event Management) to trigger immediate security alerts to IT administrators.

Print Security and IT Environment Compatibility

Printing is the most common daily task in many workplaces. An optimized printing experience is critical to maintaining productivity. At the same time, IT departments face increased demand for print security and compliance such as HIPAA and FERPA.

• Printing Standard and Compatibility

MFP compatibility with key IT environments is important for many organizations. Sharp MFPs and printers are tested and validated by major technology providers.

- WHQL-certified print driver to ensure Microsoft compatibility to meet security standard in the Microsoft environment
- Citrix-ready evaluation to ensure Sharp MFP and printer performance in the Citrix environment
- Device types to ensure printing performance in the SAP® environment
- Healthcare application compatibility including Cerner® and McKesson

Both Serverless Print Release and print retention features are available to mobile users via the Sharpdesk® Mobile application to assist with mobile print security compliance.

• User Authentication and Print Retention

When user authentication is enabled, all print jobs are authenticated and only validated print jobs are accepted on the device. In addition, with Sharp document systems, users can send print jobs and store them on the MFP's hard disk drive, which can then be securely released using a PIN number or via user authentication. It also helps minimize waste from jobs abandoned at the printer.

• Serverless Print Release

To add more convenience with security, select Sharp MFPs can be designated as a print server, and have the job released on another supported machine that is on the same network. Users can simply walk up to the most convenient printer and securely release their print jobs. It is a standard feature on select MFPs and up to five client machines can be connected for this function.

• Sharp OSA-enabled Applications

For more advanced control, Sharp and the Sharp Partner Program community offer a broad selection of tightly integrated print release and output management software, as well as advanced security features such as user authentication, authorization, and accounting. For more information, please visit the Sharp USA website.

OSA® Sharp Open Systems Architecture

Fax Security

The architecture of **Sharp MFPs provides a logical separation** between the fax telephone line and LAN, helping to **prevent attackers from gaining access** to the internal systems of the MFP or the local network. Additional security features are incorporated such as disabling broadcasting, allowing and rejecting reception from specific numbers, user authentication and more.

- Logical separation between the fax telephone line and LAN
- Only fax protocol is permitted in the fax modem
- MFP architecture is designed to minimize the risk of transmitting malicious data (virus, etc.) to the main system.
  - UART (Universal Asynchronous Receiver/Transmitter) communication on fax controller cannot control MFP controller.
  - Image transmission between fax controller and MFP controller is also separated from UART communication.

CENTRALIZED FLEET MANAGEMENT

Sharp continues to provide optimal security to its customers, immediately assessing newly discovered security threats and their impact. Security measures are often released through firmware or application updates to maximize security. In addition, intelligent management tools help monitor and optimize security and operation settings on Sharp devices.

SRDM enables administrators to take control of system features and simplify installation and management.

Sharp Remote Device Manager (SRDM)

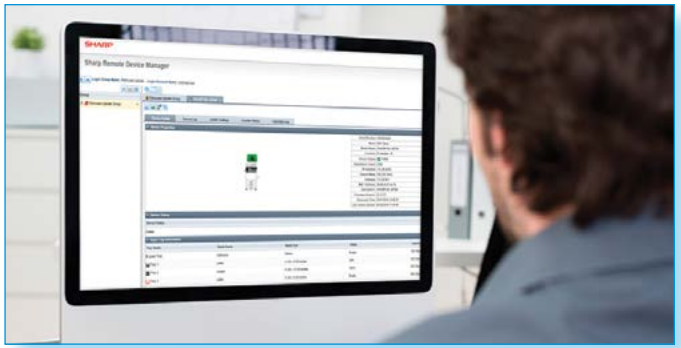
SRDM is the ideal tool for IT administrators to centrally manage, monitor and configure their Sharp MFP and printer fleets to optimize device uptime. SRDM also helps maintain optimal MFP and printer security. With this application, IT administrators can create and centrally force a custom security policy to devices on their network. If security settings are altered, SRDM will notify the administrator(s) or client incident management systems for them to immediately respond to potential security risks. SRDM can also intelligently reset security settings to the defined security policy when changes are detected. In addition, select Sharp display products can be remotely managed and monitored with SRDM V2.11 and later.*

Key Features For MFPs and Printers:

- Manual or automated device discovery
- Device status and consumable monitoring
- Security policy management
- Scheduled power management
- Centralized administrator password management
- Remote Front Panel access for quick user assistance
- Email notifications
- Firmware management
- Device cloning and storage backup
- Centralized SIEM integration
- Pre-configured driver distribution

Key Features For Display Products:

- Display device registration
- Access to device web pages
- Scheduled power management
- Remote input management
- Remote device status monitoring
- Additional device information, such as serial number



* For a complete list of supported models, please visit the SharpUSA website.

SECURITY FEATURES AT-A-GLANCE*

DATA AND INFORMATION SECURITY

Sharp MFPs provide a wide range of data security capabilities as an integral part of the device's architecture, or as a function of an optional Data Security Kit (DSK).

- Automatic Data Overwrite
- Manual Data Overwrite**
- Custom and DoD 5200.22-m
- End-of-Lease Data Erase
- Power-Up Data Overwrite**
- Up To 10-Times Data Overwrite
- 256-Bit AES Data Encryption
- Trusted Platform Module (TPM)**
- Application Whitelisting
- Self-recovery Firmware
- Data Back Up

ACCESS CONTROL SECURITY

Sharp MFPs can be configured to help provide iron-clad user access control.

- User Authentication (Local/LDAP/Active Directory)
- Group Authorization
- Active Directory Group Policy
- Page Limit Control
- Password Protected Access to Device Home Page (Administrator and User)
- User Authority Setting
- Single-Sign-On (Kerberos and OAuth Token)
- Management of Currently Logged-In Users
- USB Card Reader Support
- ID Card User Authentication
- Scan-to-Home and Scan-to-Me
- Restrict List Printing**
- Disable Destination Selection
- Disable Address Book Registration
- Receipt Rejection from Specified Sender(s)

NETWORK SECURITY

Network security with MFPs and printers is one of the most critical concerns. Sharp offers various features to help protect organizations' IT network.

- TLS Encryption (2048 bit Key supported)
- Security Policy Management
- SNMPv3 Support
- SNMP Community Name Support
- Kerberos
- IPv6 and IPsec
- Device Certificates
- IP Address Filtering
- MAC Address Filtering
- Port Control
- IEEE 802.1X™ Authentication

EMAIL SECURITY

Send to email is one of the most common tasks for document scanning. Organizations can ensure secure send to email with Sharp MFPs.

- User Authentication
- S/MIME
- Send Only to Logged in User's Email Address
- Send from Logged in User (Email Connect)
- Store Sent Email on Sent Item Folder
- Apply Exchange Email Rules to Send to Email
- Single-Sign-On (SSO) (Kerberos and OAuth token)

FAX SECURITY

(Fax option may be required)

Customers who have Sharp MFPs equipped with the fax option can be assured that the architecture of the MFP provides a logical separation between the fax telephone line and the Local Area Network (LAN).

- Segregated Fax Line
- Prevention of Junk Fax
- Confidential Fax

MOBILE AND WIFI SECURITY

Embrace mobile printing and scanning by eliminating unauthorized access to corporate network.

- User Authentication
- Print Retention
- PIN Number Printing
- Access Point WiFi Mode

DOCUMENT SECURITY

Protecting data on an MFP is only part of what's required to ensure complete end-to-end document security. Sharp MFPs employ a number of means, that if implemented, can help assure customers that their document data will remain confidential.

- Secure Print Release with a PIN Number
- Encrypted PDF (AES 256 bit Encryption)
- Encrypted PDF Lockout
- Tracking Information Print
- Hidden Pattern Print and Detection**

PRINT SECURITY

Printing is the most common use of MFPs and printers. Sharp helps protect and secure print jobs during transition and at the printer.

- User Authentication
- TLS Encryption
- Secure Print Release with a PIN Number
- Serverless Print Release
- Sharp OSA Applications

AUDIT TRAIL SECURITY

Sharp MFPs offer extensive internal logging. Audit tracking is often a critical component to monitor user and device activity. Sharp MFPs can also provide the following information:

- Job Log and Usage Tracking
- Image Job Log
- Reporting and Data Export
- Administrator System Audit Logs
- Syslog Protocol RFC 5424/3164 for Syslog/SIEM Integration
- Program Partner Applications
- SRDM Security Policy Management Features

*Color Advanced and Essentials Series MFPs. **Optional Data Security Kit Feature.

Sharp Security Suite Compatibility (**Monochrome**)

	MX-B376W/B476W MX-B376WH/B476WH	MX-M2651/M3051/ M3551/M4051/M5051/M6051	MX-M3071/M3571/ M4071M5071/M6071 MX-M3071S/M3571S/ M4071S/M5071S/M6071S	MX-M7570	MX-M905	MX-M1056/M1206 (without Fiery option)
GENERAL MFP FEATURES/FUNCTIONS						
Speed	37/47 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	75 ppm	90 ppm	105/120 ppm
Hard Disk Drive	Std	Std	Std	Std	Std	Std
Data Security Kit (DSK) & Common Criteria Certification						
Data Security Kit (optional)	MX-FR63U	MX-FR64U	MX-FR64U	MX-FR60U HCD PP (Protection Profile for Hardcopy Devices) v1.0 support	MX-FR54U HCD PP (Protection Profile for Hardcopy Devices) v1.0 support	MX-FR66U
Common Criteria Certification	Certified HCD V1.0 Dated 2015 (non-H models only)	Certified HCD V1.0 Dated 2015	Certified HCD V1.0 Dated 2015 (non-S models only)	Certified HCD V1.0 Dated 2015	-	-
Data and Information Security						
Data Overwrite (Auto)	Std	Std	Std	Std	Std	Std
Data Overwrite (Manual)	Yes	Yes	Yes	Yes	Yes	Yes
Data Overwrite At Power-up	Yes	Yes	Yes	Yes	Yes	Yes
Up To 10-times Overwrite	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 Times	Up to 7 times
Custom Overwrite Pattern	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	-
256-bit Data Encryption	Std	Std	Std	Std	Std	Std
End-of-Lease Data Erase	Std	Std	Std	Std	Std	Std
Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes	Std
Application Whitelisting	Std	Std	Std	-	-	Std
Firmware Attack Prevention & Self Recovery	Std	Std	Std	-	-	Std
Access Control Security						
User Authentication (Local Address Book)	Std	Std	Std	Std	Std	Std
User Authentication (LDAP)	Std	Std	Std	Std	Std	Std
User Authentication (Active Directory)	Std Group Policy	Std Group Policy	Std Group Policy	Std	Std	-
Group Authorization	Std	Std	Std	Std	Std	Std
Page Limit Control	Std	Std	Std	Std	Std	Std
Password Protected Access To Device Web Page	Std	Std	Std	Std	Std	Std
Restrict List Printing	Yes	Yes	Yes	Yes	Yes	Yes
Scan To Home Directory	Std	Std	Std	Std	Std	-
Scan Only To Logged-in User's Email	Std	Std	Std	Std	Std	Std
Disable Destination Method Selection	Std	Std	Std	Std	Std	Std
Disable Address Book Registration	Std	Std	Std	Std	Std	Std
Receipt Rejection From Specified User(s)	Std	Std	Std	Std	Std	Std
Lock Users After 3 Tries	Std	Std	Std	Std	Std	Std
USB Card Reader Support	Std	Std	Std	Std	Std	Std

continued on next page...

Items indicated with “Yes” in the table above may require additional options or software downloads.

Sharp Security Suite Compatibility (**Monochrome**) *continued*

	MX-B376W/B476W MX-B376WH/B476WH	MX-M2651/M3051/ M3551/M4051/M5051/M6051	MX-M3071/M3571/ M4071M5071/M6071 MX-M3071S/M3571S/ M4071S/M5071S/M6071S	MX-M7570	MX-M905	MX-M1056/M1206 (without Fiery option)
Network Security						
Active Directory Integration	Std Group Policy	Std Group Policy	Std Group Policy	Std	Std	-
TSL Encryption	Std	Std	Std	Std	Std	Std
2048 Certificate	Std	Std	Std	Std	Std	-
Security Policy Management	Std	Std	Std	Std	Std	Std
SNMPv3 Support	Std	Std	Std	Std	Std	Std
SNMP Community String Support	Std	Std	Std	Std	Std	Std
Kerberos	Std	Std	Std	Std	Std	Std
IPv6 and IPsec	Std	Std	Std	Std	Std	Std
Device Certificates	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std	Std	Std	Std	Std	Std
Port Control (Disable/Enable Ports)	Std	Std	Std	Std	Std	Std
CSRF Measure	Std	Std	Std	Std	Std	Std
Admin Password Protection*	Std	Std	Std	Std	Std	Std
IEEE 802.1X	Std	Std	Std	Std	Std	Std
SHA-2 Secure Hash Algorithm	Std	Std	Std	Std	Std	Std
S/MIME Public Key Encryption	Std	Std	Std	Std	Std	-
Fax Security (Fax Option May Be Required)						
Separation Between Fax and Network	Std	Std	Std	Std	Std	-
Confidential Fax	Std	Std	Std	Std	Std	-
Filter Junk Fax	Std	Std	Std	Std	Std	-
Document Security						
Job Status Display Only Logged-in User	Std	Std	Std	Std	Std	Std
Secure Pull Print FTP/SMB	Std	Std	Std	Std	Std	Std
Secure Print Release With a PIN Number	Std	Std	Std	Std	Std	Std
Serverless Print Release	Std	Std	Std	Std	Std	-
Encrypted PDF Transmission	Std	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	Std	Std	Std	Std	Std	Std
Hidden Security Pattern Print	Yes	Yes	Yes	Yes	Yes	Yes
Hidden Security Pattern Detection	Yes	Yes	Yes	Yes	Yes	Yes
Audit Trail and Other Security						
Job Log and Usage Tracking	Std	Std	Std	Std	Std	Std
Admin Audit Tracking (SIEM and Syslog Integration)	Std	Std	Std	Std	Std	Std
Digitally Signed Firmware	Std	Std	Std	Std	Std	-

* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage.

Items indicated with “Yes” in the table above may require additional options or software downloads.

Sharp Security Suite Compatibility (**Color**)

	MX-C300P	MX-C250/C300W	MX-C303W/C304W MX-C303WH/C304WH	MX-2651/3051/ 3551/4051/5051/6051	MX-3071/3571/ 4071/5071/6071 MX-3071S/3571S/ 4071S/5071S/6071S	MX-7081/8081 (without Fiery option)	MX-7090N/8090N (without Fiery option)
GENERAL MFP FEATURES/FUNCTIONS							
Speed	30ppm	25/30 ppm	30 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	70/80 ppm	70/80 ppm
Hard Disk Drive	-	-	Std	Std	Std	Std	Std
Data Security Kit (DSK) & Common Criteria Certification							
Data Security Kit (optional)	-	-	MX-FR61U	MX-FR62U	MX-FR62U	MX-FR55U	MX-FR58U
Common Criteria Certification	-	-	Certified HCD V1.0 Dated 2015 (non-H models only)	Certified HCD V1.0 Dated 2015	Certified HCD V1.0 Dated 2015 (non-S models only)	-	-
Data and Information Security							
Data Overwrite (Auto)	-	-	Std	Std	Std	Std	Std
Data Overwrite (Manual)	-	-	Yes	Yes	Yes	Yes	Yes
Data Overwrite At Power-up	-	-	Yes	Yes	Yes	Yes	Yes
Up To 10-times Overwrite	-	-	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 times
Custom Overwrite Pattern	-	-	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset
256-bit Data Encryption	-	-	Std	Std	Std	Std	Std
End-of-Lease Data Erase	-	-	Std	Std	Std	Std	Std
Trusted Platform Module (TPM)	-	-	Yes	Yes	Yes	Yes	Yes
Application Whitelisting	-	-	Std	Std	Std	Std	-
Firmware Attack Prevention & Self Recovery	-	-	Std	Std	Std	Std	-
Access Control Security							
User Authentication (Local Address Book)	Std	Std	Std	Std	Std	Std	Std
User Authentication (LDAP)	-	Std	Std	Std	Std	Std	Std
User Authentication (Active Directory)	-	-	Std Group Policy	Std Group Policy	Std Group Policy	Std	Std
Group Authorization	-	-	Std	Std	Std	Std	Std
Page Limit Control	Std	Std	Std	Std	Std	Std	Std
Password Protected Access To Device Web Page	-	-	Std	Std	Std	Std	Std
Restrict List Printing	-	-	Yes	Yes	Yes	Yes	Yes
Scan To Home Directory	-	-	Std	Std	Std	Std	Std
Scan Only To Logged-in User's Email	-	-	Std	Std	Std	Std	Std
Disable Destination Method Selection	-	-	Std	Std	Std	Std	Std
Disable Address Book Registration	-	-	Std	Std	Std	Std	Std
Receipt Rejection From Specified User(s)	-	Std	Std	Std	Std	Std	Std
Lock Users After 3 Tries	-	-	Std	Std	Std	Std	Std
USB Card Reader Support	-	-	Std	Std	Std	Std	Std

continued on next page...

Items indicated with “Yes” in the table above may require additional options or software downloads.

Sharp Security Suite Compatibility (**Color**) *continued*

	MX-C300P	MX-C250/C300W	MX-C303W/C304W MX-C303WH/C304WH	MX-2651/3051/ 3551/4051/5051/6051	MX-3071/3571/ 4071/5071/6071 MX-3071S/3571S/ 4071S/5071S/6071S	MX-7081/8081 (without Fiery option)	MX-7090N/8090N (without Fiery option)
Network Security							
Active Directory Integration	-	-	Std Group Policy	Std Group Policy	Std Group Policy	Std	Std
TSL Encryption	-	-	Std	Std	Std	Std	Std
2048 Certificate	Std	-	Std	Std	Std	Std	Std
Security Policy Management	-	Std	Std	Std	Std	Std	Std
SNMPv3 Support	-	-	Std	Std	Std	Std	Std
SNMP Community String Support	-	Std	Std	Std	Std	Std	Std
Kerberos	-	Std	Std	Std	Std	Std	Std
IPv6 and IPsec	Std	Std	Std	Std	Std	Std	Std
Device Certificates	Std	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std	Std	Std	Std	Std	Std	Std
Port Control (Disable/Enable Ports)	Std	Std	Std	Std	Std	Std	Std
CSRF Measure	Std	-	Std	Std	Std	Std	Std
Admin Password Protection*	-	Std	Std	Std	Std	Std	Std
IEEE 802.1X Support	-	-	Std	Std	Std	Std	Std
SHA-2 Secure Hash Algorithm	-	-	Std	Std	Std	Std	Std
S/MIME Public Key Encryption	-	-	Std	Std	Std	Std	Std
Fax Security (Fax Option May Be Required)							
Separation Between Fax and Network	-	Std	Std	Std	Std	Std	-
Confidential Fax	-	Std	Std	Std	Std	Std	-
Filter Junk Fax	-	Std	Std	Std	Std	Std	-
Document Security							
Job Status Display Only Logged-in User	-	-	Std	Std	Std	Std	Std
Secure Pull Print FTP/SMB	-	-	Std	Std	Std	Std	Std
Secure Print Release With a PIN Number	-	-	Std	Std	Std	Std	Std
Serverless Print Release	-	-	Std	Std	Std	Std	Std
Encrypted PDF Transmission	-	-	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	Std**	Std**	Std	Std	Std	Std	Std
Hidden Security Pattern Print	-	-	Yes	Yes	Yes	Yes	Yes
Hidden Security Pattern Detection	-	-	Yes	Yes	Yes	Yes	Yes
Audit Trail and Other Security							
Job Log and Usage Tracking	-	-	Std	Std	Std	Std	Std
Admin Audit Tracking (SIEM and Syslog Integration)	-	-	Std	Std	Std	Std	Std
Digitally Signed Firmware	-	-	Std	Std	Std	Yes	Yes

* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage. ** Only supports the file without a password.

Items indicated with "Yes" in the table above may require additional options or software downloads.

Sharp Security Suite Compatibility

	MX-B467P	MX-B467F	MX-B557P/B707P	MX-B557F	MX-C357F	MX-C407F	MX-C507F	MX-C407P	MX-C507P	MX-C607P
GENERAL MFP FEATURES/FUNCTIONS										
Speed	46 ppm	46 ppm	55/70 ppm	55 ppm	35 ppm	40 ppm	50 ppm	40 ppm	50 ppm	60 ppm
Hard Disk Drive (HDD)	N/A	500 GB (option)	500 GB (option)	500 GB (Std)	500 GB (option)	500 GB (option)	500 GB (Std)	500 GB (option)	500 GB (option)	500 GB (option)
Data Security Kit (DSK) & Common Criteria Certification										
Data Security Kit (optional)	-	-	-	-	-	-	-	-	-	-
Common Criteria Certification	No	No	No	No	No	No	No	No	No	No
Data and Information Security										
Data Overwrite (Auto)	Yes (DRAM only)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Overwrite (Manual)	Yes (NVRAM only)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Overwrite (Scheduled)	n/a	No	No	No	No	No	No	No	No	No
Data Overwrite (1, 3 or 7 times)	n/a	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes (with opt. HDD)
Custom Overwrite Pattern (complies with DoD)	n/a	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes (with opt. HDD)
256-bit Data Encryption	n/a	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes	Yes (with opt. HDD)	Yes (with opt. HDD)	Yes (with opt. HDD)
Out of Service Data Erase (End-of-Lease)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Element Feature (similar to TPM)	Option	Option	Option	Option	Option	Option	Option	Option	Option	Option
Application Whitelisting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Boot (similar to firmware attack prevention)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Continuous Integrity Check	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Access Control Security										
User Authentication (Local Address Book)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (LDAP)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (Active Directory)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Password Protected Access To Device Web Page	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Group Authorization	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Page Limit Control (with device quota app)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Restrict Color Printing (Permissions setting)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Restrict List Printing	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Scan To Home Directory (with scan center app)	No	Yes	No	Yes	Yes	Yes	No	No	No	No
Scan Only To Logged-in User's Email	No	Yes	No	Yes	Yes	Yes	No	No	No	No
Disable Destination Method Selection	No	No	No	No	No	No	No	No	No	No
Disable Address Book Registration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Lock Out After Failed Login Attempts (panel)	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries	1-10 tries
User Lock Out Time (panel)	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes
User Lock Out Time (webpage)	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes	1-60 minutes

continued on next page...

Items indicated with “Yes” in the table above may require additional options or software downloads.

Sharp Security Suite Compatibility *continued*

	MX-B467P	MX-B467F	MX-B557P/B707P	MX-B557F	MX-C357F	MX-C407F	MX-C507F	MX-C407P	MX-C507P	MX-C607P
Network Security										
Active Directory Integration	As printer	As printer	As printer	As printer	As printer	As printer	As printer	As printer	As printer	As printer
TLS Encryption	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
2048-bit Certificate	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Security Policy Management	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMPv3 Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMP Community String Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Kerberos	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Secure SMTP server (HTTPS)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IPv6 and IPsec	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Device and Configurable CA Certificates	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
MAC Address Filtering	No	No	No	No	No	No	No	No	No	No
Port Control (Disable/Enable Ports)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
CSRF (Cross Site Request Forgery) Counter Measure	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Admin Password Protection	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IEEE 802.1X	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SHA-2 Secure Hash Algorithm	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
S/MIME Public Key Encryption	No	No	No	No	No	No	No	No	No	No
Fax Security (Fax Option May Be Required)										
Separation Between Fax and Network	-	Std	-	Std	Std	Std	Std	-	-	-
Confidential Fax and Filter Junk Fax	-	Std	-	Std	Std	Std	Std	-	-	-
Document Security										
Job Status Display Only Logged-in User	No	No	No	No	No	No	No	No	No	No
Secure Pull Print FTP/SMB	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Secure Print Release With a PIN Number	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Serverless Print Release	No	No	No	No	No	No	No	No	No	No
Encrypted PDF Transmission	No	No	No	No	No	No	No	No	No	No
Encrypted PDF Direct Printing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hidden Security Pattern Print and Detection	No	No	No	No	No	No	No	No	No	No
Audit Trail and Other Security										
Job Log and Usage Tracking	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Admin Audit Tracking (SIEM and Syslog Integration)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Configurable Device Identify Certificate	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Digitally Signed Firmware	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Restrict Firmware Update on device	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Disable physical ports (USB, parallel, etc)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std

Items indicated with “Yes” in the table above may require additional options or software downloads.

SHARP®

SHARP ELECTRONICS CORPORATION
100 Paragon Drive, Montvale, NJ 07645
1-800-BE-SHARP • www.sharpusa.com

February 2022