Network Device Security Options

Description of Ricoh Network Security Options available for MFP and Printer Products

- **Network Port Security (ability to close unused network ports)**
  - Typically, network-enabled systems from all office equipment vendors are shipped to the customer with all the network ports "open," making it as easy as possible to add them to a customer's existing network. This practice makes network-enabled systems easy to install, unfortunately opened unused network ports pose a security risk.
  - The system administrator can enable or disable IP ports, thus controlling the different network services provided by the print controller to an individual user.
    Note: SmartDeviceMonitor for Admin resides on the client desktop and allows users to determine the status and availability of Ricoh networked peripherals. Once installed, an icon is placed on each user's desktop in the Windows Taskbar, which shows system status at a glance.
  - To provide enhanced network security, Administrators can disable a specific protocol such as SNMP or FTP using Web Image Monitor or SmartDeviceMonitor. This helps prevent the theft of user names and passwords, as well as reducing the risk of outside threats from entering the network via an unused printer or MFP port.

- **IP Address Range**
  - System administrators can restrict authorized connections to the print controller from those hosts whose IP addresses fall into a particular IP range. Commands or jobs sent from non-authorized IP addresses are ignored by the print controller.
- **WPA Support**
  - Used in conjunction with the IEEE 802.11a/b/g Wireless LAN option, WPA is a security specification that addresses vulnerabilities in wireless communications. It provides a high level of assurance to enterprises, small businesses, and even home-based users that only authorized users will be able to access their networks. *"Personal"* and *"Enterprise"* authentication and encryption features helps block intruders with wireless-enabled laptops from tapping into wireless networks to intercept data streams and passwords, or to use the wireless connection as an entry point into the customer data network.
- **802.1X Wired Authentication**
  - 802.1X provides Network-port based authentication for point-to-point communication between network devices and a LAN port. By providing a point-to-point connection to a LAN port, communication will terminate if the authentication fails.
- **SNMPv3 Encrypted Communication**
  - Simple Network Management Protocol version 3 (SNMPv3) is a network management standard widely used in TCP/IP environments. SNMP provides a method of managing network hosts such as printers, scanners, workstation or server computers, and groups' bridges and hubs together into a "community" from a centrally-located computer running network management software. It allows administrators, for example, to make changes to device settings via SmartDeviceMonitor from a networked PC with encrypted communications help to maintain a secure environment. Earlier versions (v1 and v2) of SNMP were used to configure and monitor remote devices. The latest version, SNMP v3, offers enhancements to user authentication and data encryption that deliver greater security features to protect customer data and network assets. When activated, SNMP

v3 helps prevent unauthorized users from seeing either the password and/or the actual content of the file in readable text form, protecting valuable information.

- **Kerberos Support**
  - Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by implementing secret-key cryptography. Many internet protocols do not provide any security for their passwords. Hackers employ programs called "sniffers" to extract passwords to gain access to networks. Sending an unencrypted password over a network is risky and can open the network to attack. Kerberos authentication helps to limit the risks caused by unencrypted passwords and keep networks more secure.
- **S/MIME for Scan to E-mail**
  - S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME (Multipurpose Internet Mail Extensions). MIME is an Internet Standard that extends the format of e-mail to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets.
  - This function is used to encrypt confidential data transmitted by Scan to E-mail for data protection against wiretapping.
- **Data Encryption via IPP**
  - Another method to enhance data security is through encryption. Using Ricoh's SmartDeviceMonitor for Client utility, print data can be encrypted by means of Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP), thus helping secure data between workstations and network printers/MFPs. (TLS is a protocol that helps protect privacy and data integrity between client/server applications communicating over the Internet.) Even if an attempt is made to tap print data, the intercepted data will be indecipherable. Please refer to the product specification charts for model support.