RICOH
imagine. change.

Ricoh Security Solutions

Version 15

Comprehensive and reliable solutions to protect sensitive information

Ricoh Security Solutions

Don't underestimate the risks and costs of information theft

Information is your most valuable asset. By "information" we mean classified, confidential, or otherwise sensitive documents, anything from embassy floor plans to personnel reviews. The risk of information theft is very real. For example, Verizon found in a 2011 study that some 174 million digital records were compromised by data intruders in 2011, a more than 4,000% increase over 2010.[1] Whether generated within a government, business or private setting, there is urgent need to implement effective strategies to protect information assets.

While digital technology has transformed business practices by enabling nearly instantaneous data exchange, it has brought with it some new challenges in terms of security. Specifically, those intent on undermining your interests can quickly and easily intercept information when it's in digital form. The risk can expose you to a diminished competitive advantage, possible litigation or eroding stockholder trust. Listed below are a few high-risk sectors:

High Risk Sectors	Information at Risk
Federal Government	National Security, Military and Trade Secrets
Financial	Mergers and Acquisitions, Stock Transactions
Pharmaceutical	Clinical Trials, Patent Applications, Quarterly Financial Results
General Office	Customer Lists, Executive Compensation, Restructuring Plans
High-tech	New Product Design (R&D), Intellectual Property
Laboratories	Test Methods, Research Reports
Law Firms	Briefs, Depositions, Contracts
Accounting	Audit Data, Financial Reports
Medical/Hospitals	Billing, Medical Records

Leadership in Information Security

Ricoh, a global technology company specializing in office imaging equipment, production print solutions, document management systems and IT services — is dedicated to helping you address unique and varied security challenges as they emerge. By providing customized security options for our customers Ricoh has developed a comprehensive suite of security solutions. These security solutions help protect printed and electronic data content against opportunistic or targeted threats, both internal and external.

Assessing your vulnerabilities, establishing security objectives, and taking appropriate countermeasures will help minimize the risk of potentially serious security breaches, and at the same time enable you to document your security compliance initiatives.

[1] Verizon® 2012 Data Breach Investigations Report, A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and the United States Secret Service. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

This guide details Ricoh Security Solutions that were designed to best meet your objectives when securing digital office systems. This multi-layered approach will help close the door on those that wish to exploit vulnerabilities. In fact, whether your Ricoh systems are networked or non-networked, these fully integrated, cost-efficient solutions will help guard against prevalent security breaches, without disruption to normal (authorized) document workflow.

Ricoh Security Solutions Guide

Risk Level ▶	**LOW**			**HIGH**
Security Layer	**1**	**2**	**3**	**4**
Security Objective…	• Restrict Unauthorized Device Access • Control Device Output…	Plus… • Secure Network Devices • Secure Network Print Data • Destroy Latent Data…	Plus… • Physically Secure Data/Ports • Encrypt Web Communications • Authenticate Users…	Plus… • Monitor and Control Resources • Audit All Device Activity
Ricoh Security Solutions	• User Codes • Locked Print • RAM-based Security	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • HDD Encryption • Data Encryption • DataOverwriteSecurity System • Web Image Monitor • Web SmartDeviceMonitor	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • Data Encryption • DataOverwriteSecurity System • Removable Hard Drive • Network Port Security • HDD Encryption • 128-bit Encryption over SSL/HTTPS • NT Authentication • Web Image Monitor • Web SmartDeviceMonitor	• User Codes • Locked Print • RAM-based Security • SmartDeviceMonitor • Data Encryption • DataOverwriteSecurity System • Removable Hard Drive • Network Port Security • 128-bit Encryption over SSL/HTTPS • NT Authentication • Print Copy & Control • Web Image Monitor • Web SmartDeviceMonitor • HDD Encryption • IPv6 • Kerberos • Enhanced Locked Print • Print Copy Scan (PCS) Director • Card Authentication Package

Ricoh Security Solutions

Restrict Unauthorized Device Access

User Codes
User Codes (standard in most Ricoh systems) enable system administrators to manage and track the use of Ricoh digital output devices. A User Code can be assigned to an individual based on which function(s) they have permission to access. This level of control enables you to monitor system usage (e.g., generate print counter reports by function and User Code).

Control Device Output

Locked Print
Locked Print (available through Ricoh's advanced print drivers) maintains confidentiality by suspending document printing until the authorized user (author/creator) enters the correct PIN (Personal Identification Number) from the device control panel. This eliminates the possibility of anyone viewing or removing a document from the paper tray. (Locked Print requires a hard drive that may be optional, depending on model.)

Locked Print Password Encryption
As a new feature the password used for locked printing can be encrypted to help protect against wiretapping.

Enhanced Locked Print
Enhanced Locked Print lets you capture all the benefits of shared, centralized MFPs without compromising document security. Users store, release and manage confidential documents with the security of user ID and password authorization. It's a fast and simple solution for helping to protect your organization's confidential and proprietary data.

- Users can safely send documents to printers where they are securely held until released by the authorized user.
- Documents cannot be picked up at the printer by another user, protecting information confidentiality.
- Documents stored at the printer are encrypted (information cannot be compromised if hard drive is stolen).
- Enhanced Locked Print is installed to the Multifunctional-printing device either via embedded firmware (SD Card) or remotely via Web Interface.
- Administrators and users can configure Enhanced Locked Print through a simple web browser-based interface.

RAM-based Security
Select Ricoh MFP systems use RAM (Random Access Memory) for document processing tasks as a copier, not a hard disk drive. Though a hard drive is available as an option, there is a security benefit to the base configuration in that jobs processed through RAM are volatile (i.e., when the system is turned off, data is immediately erased). Without a means to permanently store data, such as a hard drive, a key security threat is eliminated. As such, these MFP systems can be proposed for low-volume environments where information security is the top priority.

Secure Network Devices

SmartDeviceMonitor (for Admin*)
SmartDeviceMonitor is utility software bundled with all Ricoh printers, print-enabled MFPs and the Printer/Scanner Kit option. This versatile software suite simplifies all aspects of installation, monitoring and management of Ricoh network output systems, while supporting key security features.

- **Change Community Name**
  To address SNMP (Simple Network Management Protocol) vulnerability, the system administrator can change the Community Name of Ricoh hardware devices from "Public" to another more secure name. If this security measure is taken, the Community Name (for the software) must have the identical name as the connected Ricoh output device.
- **Restrict User Access**
  System administrators can control user privileges through the User Management Tool. This activates a menu for review of the peripherals authorized for use by User Code and User Name. All Ricoh supported peripherals on the network are listed, and a simple click on the device, accesses a menu that restricts or enables access to the device for individual users.

Web Image Monitor

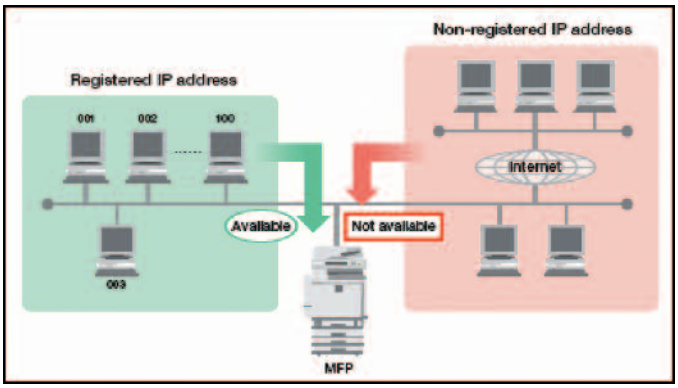
Web Image Monitor is an integrated Web-based utility for device management.

- **Set IP Address Range (IP Filtering)**
  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.
- **Network Port Security**
  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.

IP (Internet Protocol) Address Filtering

In a LAN, an IP Address is each networked computer's unique hardware number. Just like your street address with a house or apartment number, these addresses help route e-mails and attachments, forward faxes to the proper recipient, and send print data to networked output devices from originating PCs. The ability of Ricoh devices to block/restrict a particular end-user or set of end-users based on IP addresses improves the management of PCs and users, helps to balance output volumes among multiple devices, and enhances network security by limiting access to files stored in devices.

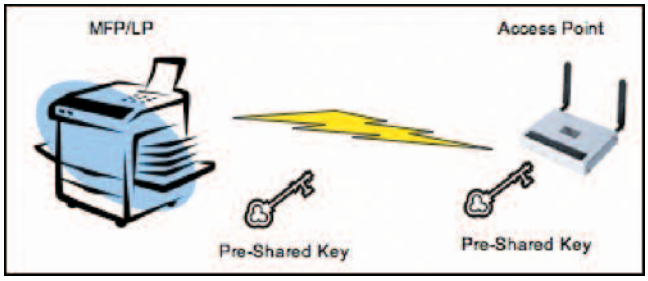


Job Logs/Access Logs

A complete listing of every job executed by the device is stored in memory. This list may be viewed via Web SmartDeviceMonitor to track and trace device usage by job and/or user. When used in conjunction with external user authentication modes, it will be possible to determine which specific users may be abusing a device. It is also possible to determine which device was used and by whom in tracing an unauthorized transmission.

WPA Support (Wi-Fi Protect Access)

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 data will remain protected by allowing only authorized users to access their networks. "Personal" and "Enterprise" authentication and encryption features block intruders with wirelessly-enabled laptops from tapping into wireless networks in any environment, preventing the interception of data streams and passwords, or from using 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.

Data Encryption

As mission critical data traverses the network it is possible for the knowledgeable hacker to intercept raw data streams, files, and passwords. The advent of wireless network technology, while increasing the convenience of surfing and printing for millions, also leaves networks vulnerable to attack from intruders armed with wireless laptops via any access points within range. Without protection, intelligible information can easily be stolen, or modified/falsified and re-inserted back into the network. Ricoh devices are equipped with the following encryption capabilities to help you reduce these risks.

Ricoh Security Solutions

Address Book Encryption

Address Book Encryption protects contact information by encrypting the data stored in a system's address book. Even if the HDD is physically removed from the unit, the data cannot be read. This function eliminates the danger of a company's or department's entire population of employees, customers, or vendors being targeted for malicious e-mail messages or PC virus contamination. Further, since address book data usually corresponds to user names and passwords used elsewhere on the network, protecting printer/MFP address book data increases overall network security.

Encrypted PDF Transmission

Adobe's PDF file format has become the universal standard for creating documents that can easily be opened and shared by any user on any platform. Adobe provides the Acrobat® Reader® application as a free download across the Web. A PDF file is essentially a snapshot of a document. It is unchangeable (although files are editable with the full Adobe Acrobat application) and therefore attractive to document owners that wish to share, but restrict alterations, to approved documents. Part of the attraction of the PDF format is that file sizes are drastically reduced versus those of the native application, making them easier and faster to e-mail.

While Adobe offers a number of security-related features within the Acrobat application to lock and password-protect documents, there is nothing to prevent the files from being intercepted in a decipherable form while traveling over the network. That's where Ricoh's Encrypted PDF Transmission function adds value, scrambling and encrypting the data that would otherwise be a very transparent document during transmission. Users may choose between 40-bit and 128-bit encryption, and set recipient rights to allow changes to or extract content from the document. (See also PDF Password Encryption.)

Hard Drive (HDD) Encryption

This function can encrypt the system's hard drive to protect against data theft. Even if the hard drive stolen, data will not be disclosed. The encryption methodology used is Advanced Encryption Standard (AES) to 256 bits.

Driver Encryption Key

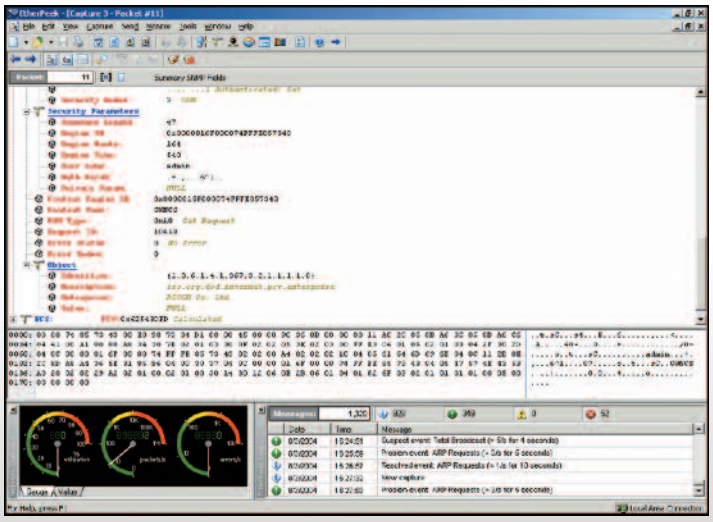
Ricoh devices offer this feature that scrambles user authentication passwords when using the PCL or RPCS drivers so others cannot access the system fraudulently using a stolen user's password.

PDF Password Encryption

This function corrects a vulnerability in Encrypted PDF Transmission in that the window for entering the user password displays the password in clear text. This function encrypts passwords up to 32 characters for more secure PDF transmission and storage. The assignment of a group password for both the destination machine and connected PCs is done via DeskTopBinder Lite.

SNMP v3 Encrypted Communication

Simple Network Management Protocol version 3 (SNMP v3) 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 to help you 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 prevents unauthorized users from seeing either the password and/or the actual content of the file in readable text form, protecting valuable information.

Kerberos

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.

IPsec Communication

IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment. Organizations that require high levels of security have networks with IPsec for data protection. These organizations require printing using IPsec.

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.

Secure Network Print Data

Data Encryption via IPP

Another powerful way to address 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 securing data between workstations and network printers/MFPs. (TLS is a protocol that helps assure privacy and data integrity between client/server applications communicating over the Internet.) This means that any attempt to tap print data will fail, i.e., the intercepted data is indecipherable. Please see the included product specification charts for model support.

Destroy Latent Data

Ricoh DataOverwriteSecurity System (DOSS):

To further thwart data loss, an organization’s information security measures should incorporate technology that destroys latent digital images on the MFP’s hard drive. Ricoh’s DataOverwriteSecurity System achieves that goal as it destroys temporary data stored on the MFP’s hard drive by writing over the latent image with random sequences of “1’s” and “0’s.”

- Ricoh’s three-pass random data overwrite process makes any effort to access and reconstruct stored print/copy files virtually impossible.
- Operates in conjunction with the Removable Hard Drive Security Systems, providing a multi-layered approach to securing sensitive documents.
- A simple display panel icon provides visual feedback regarding the overwrite process, e.g., completed or in-process.
- Conforms to National Security Agency (NSA) recommended methods of managing classified information.
- **Assists customers in their compliance with HIPAA, GLBA and FERPA requirements.**
- DOSS Type A, B, C, D, F, H and I are ISO 15408 Certified to an EAL of 3.

Security Acts Compliance Requirements

Companies that use and store certain sensitive data such as medical information, financial information or certain other information that personally identifies individuals may be subject to a number of regulatory requirements including **HIPAA (Health Insurance Portability and Accountability Act)**, **GLB (Gramm-Leach-Bliley Act)** or the **Family Education Rights Privacy Act**. While no system can absolutely assure data security, the use of Ricoh solutions such as DOSS and the RHD option can help customers address the risk posed by sensitive latent data.

Ricoh Security Solutions

Physically Secure Data/Ports

Removable Hard Drive Security (RHD) Systems
Convenient and easy to use, Ricoh's Removable Hard Drive Systems interface with a digital system's standard hard drive. This solution secures the system's internal hard drive within an external rigid housing using a key lock system. A numbered labeling system ensures the Removable Hard Drive is easy to identify while in storage or when being replaced in the system. Also provided is a cushioned static-free case to protect the Removable Hard Drive while in transit or storage.

To provide even more security and flexibility when dealing with both classified and non-classified documents, an optional additional Removable Hard Drive is available. This allows Ricoh digital systems to handle two separate interchangeable Removable Hard Drives; one RHD for classified documents and the other RHD for unclassified documents. After the classified documents have been copied or printed, the classified drive can be removed and placed in a secure location and the unclassified drive can be reinserted for unclassified copying or printing.

- The Removable Hard Drive is placed in a strategically accessible area for easy authorized removal and storage.
- Maximizes security by allowing the physical separation of data from the input/output device, preventing access to remnant data.
- Removable Hard Drive-enabled Ricoh systems operate seamlessly with the device's robust copy, print and scan features.
- Operates in conjunction with Ricoh's DataOverwriteSecurity System, providing a multi-layered approach to securing sensitive documents.
- Functions available include copy, print, scan, and Document Server* when the Removable Hard Drive is installed. When a RHD is installed the fax option is unavailable.

*__Document Server__, a capability of select Ricoh output systems that stores jobs (scan, print, fax, or copy) on the system's hard drive, also supports Secure Document Release.

Network Port Security
Typically, network-enabled systems are shipped to the customer with all the network ports "open," making the addition of these systems to different networks as easy as possible. Although making the network-enabled systems easy to install, opened unused network ports pose a security risk.

To provide enhanced network security, Administrators can disable a specific protocol such as SNMP or FTP using Web Image Monitor or SmartDeviceMonitor. This prevents the theft of user names and passwords, as well as helping address outside threats including destruction/falsification of stored data, Denial of Service (DoS) attacks and viruses that can enter the network via an unused printer or MFP port.

Encrypt Data Communication

128-bit Encryption over SSL
GlobalScan and DocumentMall both support 128-bit encryption over SSL (Secure Sockets Layer). SSL technology works by using a private key to encrypt data that's scanned from the Ricoh MFP to the GlobalScan or DocumentMall server, creating a secure connection. Any URL (Uniform Resource Locator) that requires an SSL connection, such as GlobalScan and Document Mall, will start with https:, with "s" standing for "secure."

Authenticate Users

Prevent Unauthorized System Usage:
Authentication is an MFP security feature that restricts unauthorized users, or a group of users, from accessing system functions or changing machine settings. This important capability enables the system administrator to employ "Access Limitation Management," helping to protect your MFP installed base from unapproved usage or tampering.

GlobalScan is a Web-based Content and Document Management Solution that enables select Ricoh systems to perform network scanning functions, specifically, scan to e-mail or folder, as well as perform OCR, fax and document management functions via optional plug-ins. This powerful, yet easy-to-use, paper document capture and distribution system integrates seamlessly with your existing mail infrastructure to significantly boost workgroup productivity by combining scanning functionality within an accessible copier platform. **GlobalScan's enhanced security features include:** Secure LDAP, Secure SMTP, Kerberos Authentication and Password Protected PDF.

DocumentMall, a low cost application with many security features, provides Internet access to your documents from anywhere in the world, 24 hours a day, 7 days a week, enabling easy sharing and collaboration across disperse geographic boundaries.

- **User Authentication** enables you to restrict machine access so that only those with a valid user name and password can access MFP functions.
- **Windows Authentication** verifies the identity of the MFP user by comparing login credentials (user name/password) against the database of authorized users on the Windows Network Server, thus granting or denying access to MFP functions.
- **LDAP Authentication** validates a user against the LDAP (Light-weight Directory Access Protocol) server, so only those with a valid user name/password can access your global address book, i.e., search and select e-mail addresses stored on the LDAP Server.
- **Administrator Authentication** – A registered administrator manages system settings and user access to MFP functions. Up to four Administrators can share the administrative tasks, enabling the workload to be spread and limit unauthorized operation by a single administrator, though the same individual can assume all roles. In addition, a separate Supervisor can be established for setting or changing the administrator passwords.
- **Basic Authentication** – Authenticates a user utilizing the user name/password registered locally in the MFP's Address Book. No one without a valid user name/password can access the machine.
- **User Code Authentication** – Utilizes Ricoh's standard User Code system to authenticate the user. The MFP operator simply enters their User Code, which is compared to the registered data in the MFP's address book. No one without a valid User Code can access the machine.

  Basic Authentication and User Code Authentication can be utilized in non-Windows and/or non-networked office environments.
- **US Department of Defense Common Access Card (CAC) Authentication** – The Common Access Card (CAC) is a US DoD specialized ID card-based authentication system design for government users that must be compliant with the Homeland Security Presidential Directive -12 (HSPD-12). This Directive requires that all federal employees and contractors enhance security efficiently by reducing identity fraud through increased protection of personal privacy. The only customers for Ricoh's CAC Authentication Solution is the U.S. Department of Defense (DoD) [US Army, Navy, Air Force, Marines, Coast Guard and affiliated agencies].
- **Personal Identity Verification (PIV)** is the civilian U.S. government version of the CAC card.

Monitor and Control Resources

Print Copy Scan (PCS) Director

Print Copy Scan (PCS) Director is a comprehensive print management solution, which enables customers to analyze, understand and ultimately save on the costs associated with printing and photocopying. This solution can be implemented to silently monitor printing activity, limit the number of prints and copies a user can make, as well as enforce "rules based" printing methodologies to reduce Total Cost of Ownership.

Print Copy Scan (PCS) Director identifies and controls the cost of printing across the entire enterprise.

Audit All Device Activity

Ricoh Print and Copy Control v3 for Equitrac Office and Express

Ricoh Print and Copy Control enables customers to better control user access and track copy/print information via software embedded onto the hard disk drives of select Ricoh output systems. Advantages include:

Secure Authentication Options

Protect sensitive data and prevent unauthorized use with the authentication method that fits your business.

- Ultimate simplicity and security. Employees access MFPs using their company ID badges and optional card readers that install in minutes. Ricoh PCC accepts MIFARE®, Legic®, HID® Prox (125 KHz) and magnetic stripe cards.
- Convenient customized access. Easily track all document output using secure PIN access — by user, project or even workgroup.
- Instant company-wide access. Users simply input their existing network IDs and passwords to "unlock" MFPs.

User Friendly and Secure

- Convenient, secure printing. Follow-You™ document production lets you output documents from any network MFP so you can avoid busy or unavailable machines, or send multiple documents and print them as needed in different departments, floors or buildings.
- Timed control. Administrators can schedule automatic deletion of jobs from the server after a preset time limit.
- Strengthened security. Jobs reside on a secure server — not on system hard drives. Plus, fewer documents sit unattended in output bins since they're held until released by user.

Ricoh Security Solutions

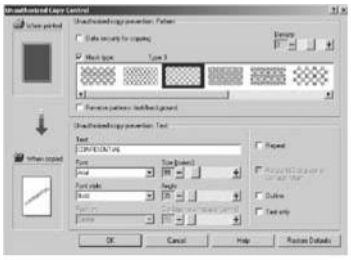
Unauthorized Copy Control

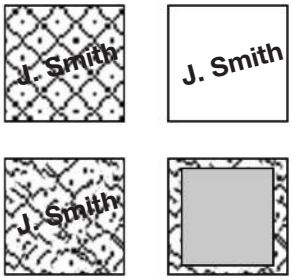
Ricoh's print driver supports a unique feature that no other manufacturer offers, Unauthorized Copy Control. What this feature does is embed patterns and text under printed text to help eliminate the risk of unauthorized copying of sensitive documents.

This new functionality is ideal for smaller businesses that primarily use the system for fax, copy and print output, for instance, companies that copy personnel reports, compensation plans, medical records, financial reports, etc.

Unauthorized Copy Control consists of two functions:

1. Mask Type for Copying[2] is a standard feature that embeds a masking pattern and message within the original printout. If copies are made, either on the Ricoh or competitive digital systems, the embedded message appears; the author's name, for instance, would help identify the originator.





Masked Type for Copying

Data Security for Copying

2. Select Data Security for Copying[1] all copy output that is made on a MFP equipped with the Copy Data Security Unit will be grayed out, leaving only a 0.16" (4mm) margin of masking pattern.

Notes:

[1] Requires optional Copy Data Security Unit. Not supported on some Fax-enabled configurations. Copy reduction ratio less than 50% will be deactivated.

[2] Some digital MFPs may not detect masking patterns.

Mandatory Security Information Print

Mandatory Security Information Print is a feature that includes information about who printed the document, when and from which device.

Types of security information that will be included with Mandatory Security Information Printing:

- Date and Time when the job was printed
- Name or Log-in User ID of the user who printed the job
- IP address of the device which printed the job
- Serial number of the device which printed the job

Administrators can select which types of information should be printed on the output. The print position can be changed to upper left, upper right or lower left. (Default setting: lower right)

General Office Commercial Facsimile Security Features

Standalone Commercial Fax

Restricted Access
Restricted Access allows you to keep close track of machine usage and deters passers-by from using the machine. Authorized users must enter a code before they can use the machine. Furthermore, this function can be linked to the Night Timer feature so that Restricted Access is turned on/off at certain hours, preventing after-hours access.

Server Domain Authentication
When security and user tracking are an issue for IT Managers, Server Domain Authentication is standard on the FAX4420NF and FAX5510NF. Authentication limits access to the fax systems increasing security by monitoring machine usage. Machine access is given only to users with a Windows domain controller account. Server Authentication will limit access to the fax system not only for scan to e-mail, but also for standard faxing, IP faxing and LAN faxing.

Security PIN Code Protection
To prevent exposure of a PIN Code or Personal ID, any character after a certain position in the destination's dial number will be concealed both in the display and Communications Report.

Closed Network
With Closed Networks, the ID codes of the communicating machines are checked. If they are not identical, the communication is terminated, thus preventing possibly confidential documents from being transmitted intentionally or accidentally to the wrong location(s), i.e., outside the network. (Note: Closed Network requires all fax systems be Ricoh systems with closed network capability.)

Confidential Transmission/Reception
This feature enables the user to transmit/receive to a mailbox that is passcode-protected. Messages are only printed after the recipient enters the proper passcode, providing an enhanced level of security when communicating between machines.

Memory Lock
When Memory Lock is enabled, documents from all senders (or specific senders) are retained in memory. When the Memory Lock ID is entered from the control panel, the documents print, another form of security that prevents documents from sitting on a receive tray for passers-by to read.

Networked Commercial Fax

ITU-T Sub-address Routing
Using a Sub-address, appended to a fax number, makes it possible to route a fax directly to the recipient's PC, via their e-mail address. When received to a PC, confidentiality is maintained, i.e., only the recipient can view the message.

IP-fax
Ricoh Facsimile Systems, with NIC FAX Unit installed, support secure T.38 real-time IP-fax over a corporate Intranet, not only bypassing costly phone lines, but also operating securely behind the firewall.

Ricoh Security Solutions Compatibility Chart

	Commercial Facsimile Security Features							
	Closed Network	Confidential Transmission/Reception	IP Fax	ITU-IT Sub-address Routing	Memory Lock	Restricted Access	Security PIN Code Protection	Server Domain Authentication
Super G3 Facsimile								
FAX 1190L					■	■		
FAX3320L	■	■			■	■	■	
FAX4430L	■	■			■	■	■	
FAX4430NF	■	■	■	■	■	■	■	■
FAX5510L	■	■			■	■		
FAX5510NF	■	■	■	■	■	■		■

Ricoh Security Solutions

ISO 27001 Information Security Statement

ISO 27001:2005 is an auditable international standard setting out the requirements for an Information Security Management System (ISMS). The standard is designed to identify, manage, and minimize a wide range of threats to which information is regularly subjected, and requires that processes and procedures are scripted to identify and minimize security risks that may affect information systems.

Ricoh recognizes the importance of helping to protect the information assets of our business, our customers, our business partners, and our employees. Ricoh is committed to developing, implementing, and continually improving our ISMS to identify and protect the information assets of our business operations. Ricoh has chosen the ISO 27001 standard and certification in key locations and departments to demonstrate our commitment to information security.

ISO 27001:2005
The ISO 27001 International Standard, published in 2005, sets out the requirements for Information Security Management Systems. It is supplemented by ISO/IEC 17799:2005 (Information Technology — Security techniques — Code of practice for information security management). The code of practice is a reference document which defines best practices for information security management, and is a direct outgrowth of the earlier British Standard BS 7799.

Ricoh IEEE 2600.1/ISO 15408 Certification Statement

IEEE 2600.1/ISO 15408 Certification
IEEE 2600.1 is an information technology security standard developed by the office equipment industry. The standard defines the minimum requirements for security features used by Multifunctional Products (MFPs) in operational environments that require a high level of document security. The industry accepted, independent third-party verification offered via ISO 15408 security testing is combined with a fixed protection profile to provide a common baseline for assessing MFP security. MFPs achieving certification for the IEEE 2600.1 standard are designed with enhanced security features to conform to the established protection profile. To ensure that the MFP demonstrates conformance with the established standard, an independent third-party laboratory tests and provides verification that a vendor's security features claims are accurate and issues a validation report. Customers can then use the IEEE 2600.1 validation reports issued for the certified or compliant MFP in their own information security plans to demonstrate that reasonable effort has been made to safeguard information.

Key features, benefits and offerings to our customers

- Validation of MFP security features by an independent third party laboratory that is recognized by the US Government
- Independent third-party verification that a vendor's security features claims regarding its MFPs are accurate
- A comprehensive standard establishes a common baseline of security expectations for MFP products
- No longer need to evaluate individual security feature claims from different vendors
- Customers can use the information generated by the certification testing as a proof source for their information security plans

Areas of the MFP that have been tested to the IEEE 2600.1 Standard
The following MFP functional areas have been validated to the IEEE 2600.1 standard. These areas have been identified as the most vulnerable for possible data breach.

- User Identification and Authentication systems
- Data Encryption technology available for the MFP systems
- Validation of the MFP system's firmware
- Separation of the analog fax line and copy/print/scan controller
- Validation of the data encryption algorithms
- DOSS Operation

Product Certification Statement
Ricoh Americas Corporation has a dynamic and evolving product offering. Please visit http://www.ricoh.com/about/security/products/mfp/cc/ for the most up-to-date product certification information.

Ricoh is a forward looking company with a dynamic product line constantly being improved to meet our customers changing requirements. IEEE P2600.1/ISO 15408 Certification for Ricoh products is a constant process with ongoing certification updates and efforts. This being said the latest certification information may not be listed on this website. Please contact your Ricoh sales professional for the most up-to-date information regarding IEEE P2600.1/ISO 15408 Certification.

Ricoh Security Solutions

Ricoh Security Solutions Compatibility Charts

	Network Protection			Device Access									Data Encryption									Document Protection								Security Certs.
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option	Mandatory Security Information Print	IEEE 2600.1/ISO 15408 Certification
Color Multifunction																														
Aficio MP C6501/ C7501	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■					
Pro C550EX/ C700EX*	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■		
Pro C900s	■	■	■	■	■	■	■	■					■	■	■		■		■	■			■									
Aficio MP C300/SR/ C400/SR	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■						
Aficio MP C3001/ C3501	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■					■	
Aficio MP C4501/ C5501	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■					■	
Aficio MP C2051/ C2551	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	
Aficio MP C305SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
Aficio MP C3502/ C3002 SPF	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Aficio MP C5502/ C4502 SPF	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Aficio SP C242SF	■	■	■	■				■												■		■				■						

** Note: The Pro C550EX/Pro C700EX and Fiery controllers have separate security features. The security features listed above are for the mainframe GW controller only. If the mainframe is configured with the Fiery, the Fiery's security features take precedence.*

	Network Protection			Device Access										Data Encryption										Document Protection										Security Certs.
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option	Mandatory Security Information Print	IEEE 2600.1/ISO 15408 Certification
Black & White Multifunction																																		
Aficio SP 4100SFL/ SP 4100SF/SP 4110SF	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■		
Aficio MP 171/F/ SPF	■	■	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[2]	■[1]	■[1]		■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■						
Aficio MP 2851SP/ MP 3351SP	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■						
Aficio MP 4001SP/ MP 5001SP	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■					
Aficio MP 4000B/ 4000/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■		
Aficio MP 5000B/ 5000/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■		
Aficio MP 6001/ 7001/8001/9001	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■		
Pro 907EX/1107EX/ 1357EX	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■		
Aficio MP 201F/ 201SPF	■	■	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[2]	■[1]	■[1]		■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■			■	■		
Aficio SP 5200S/ 5210SF/5210SR	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■		■		
Aficio SP 1200SF																										■						
Aficio MP 301SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
Aficio SP 3400/ 3410 SF	■	■	■																					■		■						
Aficio SP 3510 SF	■	■	■																	■				■		■						
Aficio SP 4410SF (SFgx)	■	■	■	■	■	■	■					■									■		■	■		■						
Aficio MP 2352/ 2852/3352 SPF	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■							■
Aficio MP 5002/ 4002/SPF	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Aficio MP 6002/ 7502/9002 SPF	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	

[1]*Printer/Scanner Kit is required.* [2]*Printer/Scanner Kit and IEEE 802.11b required.*

Ricoh Security Solutions

	Network Protection			Device Access									Data Encryption									Document Protection								Security Certs.
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option	Mandatory Security Information Print	IEEE 2600.1/ISO 15408 Certification
Color Printers																															
Aficio SP C231N/ C232DN	■	■	■																						■						
Aficio SP C420DN	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■		
Aficio SP C420DN-KP HotSpot	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■		
Aficio SP C820DN	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■		
Aficio SP C821DN	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■		
Aficio GX2500	■	■																								■						
Aficio GX3000*	■	■	■	■		■																				■		■				
Aficio GX e3300N*	■	■	■	■		■																				■		■				
Aficio GX3050N*	■	■	■	■		■																				■		■				
Aficio GX e3350N*	■	■	■	■		■																				■		■				
Aficio GX5050N*	■	■	■	■		■																				■		■				
Aficio GX e5550N*	■	■	■	■		■																				■						
Aficio GX7000	■	■																								■						
Pro C900	■	■	■	■	■	■	■	■					■	■	■		■		■	■			■									
Aficio SP C430DN/ SP C431DN	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■	■						
Aficio SP C431DN-HS	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■							
Aficio GX e7700N	■	■	■	■		■																				■						
Pro C651EX/C751EX	■	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■		■		■							

GX3000/3050N/5050N does not use the same Web Image Monitor as the other Ricoh printers. The browser is developed by Silex Technology and will be slightly different from the other models.

**The GX3000/GX e3300N/GX3050N/GX e3350N/GX5050N/GX e5550N support "IP address filtering" feature only. "Mac address filtering" is not supported. Locked/Secure Print is only available if the Hard Disk is installed*

	Network Protection			Device Access										Data Encryption										Document Protection									Security Certs.
	Web Image Monitor	SmartDeviceMonitor	Network Protocols ON/OFF	Administrator Authentication	Job Log/Access Log	IP Address Filtering	User Account Registration	User Authentication	Wi-Fi Protect Access (WPA)	Kerberos	802.1X Wired Authentication	U.S. DoD Common Access Card (CAC) Auth.	128-bit Secure Socket Layer (SSL)	Address Book Encryption	Encrypted PDF Transmission	Driver Encryption Key	PDF Password Encryption	SNMP v3 Encryption	S/MIME for Scan to Email	IPsec Communication	HDD Encryption	Locked Print Password Encryption	DataOverwriteSecurity System (DOSS)	Locked/Secure Print/Enhanced Locked Print	Password Protection of Stored Documents	RAM-based Security* (If Hard Drive is Optional)	Removable Hard Drive	Unauthorized Copy Control	Mask Type for Copying	Copy Data Security Option	Mandatory Security Information Print	IEEE 2600.1/ISO 15408 Certification
Black & White Printers																																
Aficio SP 3300D/ SP 3300DN	■	■	■																						■							
Aficio SP 4100NL	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■		
Aficio SP 4100N-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■			
Aficio SP 4110N-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■		
Aficio SP 4210N	■	■	■				■	■	■		■		■					■		■			■	■		■		■	■	■		
Aficio SP 5100N	■	■	■			■	■	■					■		■		■									■						
Aficio SP 6330N	■	■	■	■	■	■			■																	■		■				
Aficio SP 8200DN	■	■	■	■	■		■	■	■					■				■		■	■	■	■	■	■	■		■	■	■		
Aficio SP 9100DN	■	■	■			■	■	■	■				■		■		■						■	■	■		■	■				
Aficio SP 5200DN	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■		■						■						
Aficio SP 5210DN	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■	■	■	■	■							
Aficio SP 1210N																										■						
Aficio SP 4310N	■	■	■		■		■	■	■		■		■	■			■	■		■	■		■	■		■		■	■	■		
Aficio SP 1210N	■	■	■																					■		■						
Aficio SP 3400n/ SP 3410D	■	■	■			■	■																	■		■						
Aficio SP 3510DN	■	■	■			■	■																	■		■						

The content of this document, and the appearance, features and specifications of Ricoh products and services are subject to change from time to time without notice. Products are shown with optional features. While care has been taken to ensure the accuracy of this information, Ricoh makes no representations or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Your actual results, including print speed and other performance measures, will vary depending upon your use of the products and services, and the conditions and factors affecting performance. THERE ARE NO GUARANTEES THAT YOU WILL ACHIEVE RESULTS SIMILAR TO OURS. RICOH DOES NOT PROVIDE LEGAL, TAX, ACCOUNTING OR AUDITING ADVICE, OR REPRESENT OR WARRANT THAT OUR PRODUCTS OR SERVICES WILL GUARANTEE OR ENSURE COMPLIANCE WITH ANY LAW, REGULATION OR SIMILAR REQUIREMENT. Customer is responsible for making the final selection of products, solutions and technical architectures, and for ensuring its own compliance with various laws such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

RICOH
imagine. change.

www.ricoh-usa.com

Ricoh Americas Corporation, 70 Valley Stream Pkwy, Malvern, PA 19355, 1-800-63-RICOH
Ricoh® and the Ricoh logo are registered trademarks of Ricoh Company, Ltd.
Windows and Windows 3.1/95/98/Me/NT 4.0/2000/XP are registered trademarks of Microsoft Corporation.
All other trademarks are the property of their respective owners. Print speed may be affected by network, application or PC performance. Specifications and external appearances are subject to change without notice.