

Ricoh Aficio Common Security Features Guide

SECURITY SOLUTIONS

Color Multifunction Devices
Black & White Multifunction Devices
Color Printers
Black & White Printers
Super G3 Facsimiles



*Maintaining data security in
networked environments for
ultimate customer peace of mind*

RICOH

Version 11

Ricoh Aficio Common Security Features Guide

TABLE OF CONTENTS

| | |
|--|-------|
| Introduction..... | 1 |
| Information is an Asset..... | 1 |
| Risk Levels..... | 4 |
| Ricoh Aficio Security Solutions Compatibility Chart..... | 4 |
| Ricoh Security Solutions Review..... | 6 |
| Network Protection..... | 6 |
| Web Image Monitor..... | 6 |
| SmartDeviceMonitor..... | 6 |
| Network Protocol ON/OFF..... | 7 |
| Device Access..... | 7 |
| Administrator Authentication..... | 7 |
| User Authentication..... | 8 |
| Common Access Card (CAC) Authentication..... | 9 |
| IP Address Filtering..... | 9 |
| Job Logs / Access Logs..... | 9 |
| User Account Registration..... | 10 |
| Wi-Fi Protect Access (WPA) Support..... | 10 |
| Kerberos..... | 10 |
| 802.1x Wired Authentication..... | 10 |
| Data Encryption..... | 11 |
| 128-bit Secure Socket Layer (SSL) Support..... | 11 |
| Address Book Encryption..... | 12 |
| Encrypted PDF Transmission..... | 12 |
| Driver Encryption Key..... | 13 |
| PDF Password Encryption..... | 13 |
| SNMP v3 Encrypted Communication..... | 13 |
| S/MIME for Scan to E-mail..... | 13 |
| IPsec Communication..... | 13 |
| Hard Disk (HDD) Encryption..... | 14 |
| Document Protection..... | 14 |
| Hard Disk Drive Data Protection (DOSS)..... | 14 |
| Locked Print/Secure Print..... | 15 |
| Locked Print Password Encryption..... | 15 |
| Enhanced Locked Print..... | 15 |
| SmartDeviceMonitor (for Admin)..... | 16 |
| Password Protection of Stored Documents..... | 16 |
| RAM-based Security..... | 17 |
| Removable Hard Disk Drive..... | 17 |
| Unauthorized Copy Control/Masked Type..... | 17 |
| Commercial Facsimile Security Solutions..... | 18 |
| Closed Network..... | 19 |
| Confidential Transmission/Reception..... | 19 |
| IP-fax..... | 19 |
| ITU-T Sub-address Routing..... | 19 |
| Memory Lock..... | 19 |
| Restricted Access..... | 19 |
| Security PIN Code Protection..... | 19 |
| Server Domain Authentication..... | 20 |
| Wrong Connection Prevention..... | 20 |
| Fax Security Compatibility Table..... | 20 |
| Security Solution Compatibility Tables..... | 21-24 |

Ricoh Corporation
Five Dedrick Place
West Caldwell, NJ 07006

Specifications subject to change without notice.
©2009, Ricoh Americas Corporation.

This guide is intended solely for the use and information of Ricoh Americas Corporation, its designated agents, and their employees. The information in this guide was obtained from several different sources that are deemed reliable by all industry standards. To the best of our knowledge, this information is accurate in all respects. However, neither Ricoh Americas Corporation nor any of its agents or employees shall be responsible for any inaccuracies contained herein.

Windows® and Windows® 95/98/Me/NT4.0/2000/Server 2003/Vista are registered trademarks of Microsoft Corporation. Macintosh®, Mac® OS, and AppleTalk® are registered trademarks of Apple Computer, Inc. Adobe® and PostScript® are registered trademarks of Adobe Systems, Inc. PCL® is a registered trademark of Hewlett-Packard Company. Ricoh® and Aficio® are registered trademarks of Ricoh Company, Ltd. RPCS™ is a trademark of Ricoh Company, Ltd. All other trademarks are the property of their respective owners and are hereby acknowledged.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the Publisher.

Ricoh Aficio Common Security Features Guide

INTRODUCTION

Information is an Asset

Did you know that 90% of all corporate espionage is conducted by someone within the organization, a trusted employee in or near a position of power with seemingly impeccable credentials?

Motives range from monetary gain to emotional revenge but the result is the same: information a company deems classified or personal is used against it in an effort to disrupt business. Depending upon the severity of the leak and the financial investment involved, the results can be devastating. Stealing secrets is not uncommon in today's ultra competitive business culture, where being the first to market with a new technology or leapfrogging a competitor's current capabilities, if only for a few months, can have dramatic impact on the bottom line. Consider these real life business examples¹:

- Recently a New Jersey electronics firm executive was charged with breaking into a competitor's network and attempting to steal its customer and supplier lists in an effort to undercut their pricing to win business.
- In 2004 a man was arrested for trying to sell blueprints needed to repair aircraft engines that were stolen from a U.S. company to another country.
- In 2003 two men were charged with stealing and selling company secrets from an auto parts manufacturer.
- Theft is not limited to paper-based or electronic information. In 2005, a scandal erupted at Atlanta-based Coca-Cola Co. when the assistant to the global brand director was accused of stealing documents as well as *an actual sample of a new beverage formula under development* and trying to sell them to rival Pepsi.

It seems like every week we hear another instance of subscriber lists, credit cardholder files, or medical records being stolen ostensibly for identify theft purposes. Even the federal government's top secret Los Alamos lab has suffered security breaches with entire laptops disappearing. And we haven't even touched on the highest profile security application: military and government agencies and contractors. Yet, the truth is all the protection in the world may not stop a network-savvy thief who is determined to engage in espionage. But these threats can be minimized.

Recognizing the dangers that exist, (and in some cases via painful firsthand experiences), device access and data security has quickly moved to the top of the list of customer concerns and purchase criteria. However, protecting information can be expensive. Threats are everywhere and each time one loophole is closed, another opens. For example, left unchecked, employees can scan and send data to any network address, or copy data directly to portable CDs or thumb drives. Hackers present a constant threat to corporate networks, while the convenience of wireless connectivity has simultaneously opened another window of vulnerability into the corporate network. Companies today spend an incredible amount of their time, money, and resources performing risk assessments and securing their information systems.

The bottom line: Data is inert. It cannot move, change, be copied, or erased without some sort of human manipulation or instruction. That is why even the most well conceived security plan is subject to some risk when the workflow involves variables including people, paper, multiple devices, and worker habits and their motives.

¹Cited examples from "Cola caper points up need for toughened safeguards," published in Arizona Republic, courtesy of Associated Press, August 2005.

Perhaps you've read the John Grisham novel *The Firm*, or have seen the movie by the same title. In it, the trusted attorney turns against his employers. He circumvents the modest document security features by having an assistant copy legal files after hours by means of stolen magnetic swipe cards that are used to track and bill clients for chargeback purposes. That was fiction, but based on real-world experiences. Today's threats are more complex, involving multiple media. This table identifies several high-risk sectors that without adequate protection of data streams and stored documents leave companies vulnerable to information theft, leaking, or falsification.

| High Risk Sectors | Information at Risk |
|---------------------------|---|
| Federal Government | National Security, Military, and Trade Secrets, Social Security, Veteran's Administration Data |
| Financial | Mergers and Acquisitions, Stock Transactions |
| Pharmaceutical | Clinical Trials, Patent Applications, Quarterly Financial Results |
| General Office | Customer Lists, Executive Compensation, Restructuring Plans, Employee Reviews, Product Launch/Pricing 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, Patient Medical Records |

Ricoh Aficio Common Security Features Guide

To help combat these problems, the federal government has enacted several pieces of legislation. These bills at once hold companies accountable for the records they keep, give businesses and individuals legal recourse in the event of damages, and also present significant security challenges to an already overburdened IT staff. They must proactively address security concerns that impact the applications, databases, and other business assets essential to daily operations while keeping up with regulations such as the HIPAA and Gramm-Leach-Bliley Acts that require firms to protect their confidential information. As a result, IT administrators, Chief Security Officers and business managers are forced to constantly re-examine their networks and business processes to make certain they are still in compliance.

Government Legislation Impacts Security Compliance

Security adds a new dimension to document workflows, especially those that involve intellectual property or deal with information that is regulated by new government standards. These pieces of legislation have forced companies to adopt practices that safeguard both business and personal information:

- **The Health Insurance Portability and Accountability Act (HIPAA)** is a law designed to protect workers from hiring discrimination based on pre-existing medical conditions. It means medical practitioners and healthcare-related companies cannot release your information without your approval.
- **The Gramm-Leach-Bliley Act (GLBA)** is a law that allowed commercial and investment banks and insurance companies to consolidate. It includes a Financial Privacy Rule that demands companies protect personal customer information and inform you if and when that information is to be shared.
- **The Family Educational Rights and Privacy Act (FERPA)** is a law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records, and requires written permission to release student information.

As you can see the need to protect data is not just for personal or even business interests, it's the law. As you'll learn, the entire family of Ricoh office solutions is equipped with a mix of features and capabilities that assist in compliance with these government regulations.

Risk Levels

Every company is different and their exposure to all types of security threats will vary based on the nature of their business and the sensitivity of the information that is processed. Further, the location and configuration of a specific device will also impact the appropriate level of security. Non-networked devices, for example, may only require local (internal) user authentication whereas networked peripherals will demand more robust login (external) controls. Those devices with hard disk drives used for long-term document storage require different security solutions than a desktop printer that uses only RAM to temporarily store print jobs. This table identifies the measures a customer can implement based on their objectives.

| Risk Level | Low High | | | |
|-------------------------------------|---|---|---|--|
| Security Layer | 1 | 2 | 3 | 4 |
| Security Objectives: | <ul style="list-style-type: none"> Restrict Unauthorized Device Access Control Device Output | <i>Plus...</i> <ul style="list-style-type: none"> Secure Network Devices Secure Network Print Data Destroy Latent Data | <i>Plus...</i> <ul style="list-style-type: none"> Physically Secure Data/Ports Encrypt Web Communications Authenticate Users | <i>Plus...</i> <ul style="list-style-type: none"> Monitor and Control Resources Audit All Device Activity |
| Available Security Controls: | <ul style="list-style-type: none"> Local Authentication (User Codes) Locked Print RAM-based Security HDD Encryption | <ul style="list-style-type: none"> Local Authentication (User Codes) Locked Print RAM-based Security SmartDeviceMonitor Data Encryption DataOverwrite-Security System Web Image Monitor Web SmartDevice-Monitor HDD Encryption | <ul style="list-style-type: none"> Local Authentication (User Codes) Locked Print RAM-based Security SmartDeviceMonitor Data Encryption DataOverwrite-Security System Removable Hard Drive Network Port Security 128-bit Encryption over SSL/HTTPS Network Authentication (Windows, LDAP) Web Image Monitor Web SmartDevice-Monitor IPv6 Kerberos | <ul style="list-style-type: none"> Local Authentication (User Codes) Locked Print RAM-based Security SmartDeviceMonitor Data Encryption DataOverwrite-Security System Removable Hard Drive Network Port Security 128-bit Encryption over SSL/HTTPS Network Authentication (Windows, LDAP) Unauthorized Copy Control/Masked Type for Copying Web Image Monitor Web SmartDevice-Monitor HDD Encryption IPv6 Kerberos Enhanced Locked Print Print Director Card Authentication Package |

Ricoh Aficio Common Security Features Guide

No matter how light or severe each customer regards company security requirements, their areas of concern and your solutions with respect to installing office equipment on their network generally fall into four categories.

- **Network protection.** How can the company safeguard its overall information infrastructure? Can you be sure the new device won't be used as a gateway for hackers? How can you help alleviate the installation and monitoring burden on IT personnel?
- **Local device access and user authentication.** How can you ensure only authorized people can access the device? What measures are in place to protect system settings, passwords, and documents stored in device memory?
- **Data and document encryption.** As files and passwords travel over the network, what is to stop them from being intercepted, especially in wireless environments?
- **Document protection.** Once data is stored at the device, how is it kept secure, and once deleted, is it gone forever? How can your customers be sure? What if the device is to be relocated elsewhere in the company, or returned at end-of-lease?

To address these and other concerns, Ricoh equips its products with an array of standard and optional features to limit device access, track usage, and protect confidential information stored in memory. Some are very basic, like the Locked/Secure Print mode available on most drivers. Some are optional based on device type (MFP versus printer via the control panel functionality inherent in each device); others are enabled only on color versus monochrome devices. Web SmartDeviceMonitor allows some security-related features like IP Address Filtering to be applied to all devices on the network simultaneously. There is even one feature that provides security through the absence of a capability. RAM-based Security is a term that applies to systems that do not have a hard disk drive or have one as an option. All data processing is executed by RAM, and when the power is turned off, all data is immediately erased. Without a means to permanently store data, the security threat is eliminated. If you think that this is a meaningless "feature by default," consider that a large customer recently purchased several thousand low-volume Ricoh digital MFPs expressly because they did not have a hard disk.

On the following pages you will find reviews of the various Ricoh security-related features and software utilities available for use with Aficio MFPs, printers, and faxes. A Ricoh Aficio Security Solution Compatibility Chart is included at the end of the section for at-a-glance convenience. Use this information to position your Ricoh solutions as devices that help protect vital intellectual property against both internal and external threats, and maintain compliance with rigorous security requirements and legislation.

Ricoh Aficio Common Security Features Guide

- **Change Community Name:** To address SNMP (Simple Network Management Protocol) vulnerability, the system administrator can change the Community Name of networked hardware devices from “Public” to another more secure name. If this security measure is activated, 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. In this way administrators can block Marketing users from accessing the Human Resources MFP hard drive, for example.

Network Protocol ON/OFF

Typically, network-enabled systems are shipped to the customer with all the network ports “open,” making the integration of these systems across different network types as easy as possible. While making network-enabled systems easy to install, unused open network ports also 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 eliminating outside threats including destruction/falsification of stored data, Denial of Service (DoS) attacks, and viruses from entering the network via an unused printer or MFP port.



Device Access

Device Access refers to the features and utilities that impact whom as an end-user can copy/print/scan/send, and who as an IT administrator can set rules for device use. Let's begin with getting permission to use the device—authentication—and then proceed to other features that track and trace usage.

Administrator Authentication

Allows a System Supervisor to set the level of device access rights for System Administrators based on their roles and responsibilities, preventing unauthorized administrators from changing system or network settings beyond their level of assigned access rights, or geography. An individual may be assigned one or more of the following roles:

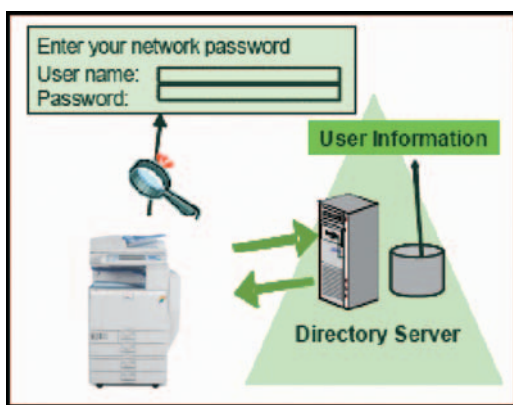
| | |
|------------------------------|---|
| Machine Administrator | Limits administrator rights to changing the machines' default settings. |
| Network Administrator | Adds network settings to features that administrators can access in addition to above. |
| File Administrator | Gives the administrator rights to access files stored in the device. |
| User Administrator | Allows an administrator to register and modify data stored in system address books. |
| Supervisor | The Supervisor role does not directly manage devices, but instead controls passwords and the level of access rights assigned to each administrator, as described above. |

User Authentication

Several modes of user authentication are available to ensure only authorized personnel issued a valid user name and password has access to the device and the data stored within it. There are two types of authentication, **External**, which uses information from a remote server to verify users, and **Internal**, which identifies users by data stored locally in the machine. As a result, the types of authentication available to users will vary based on how the device is installed, networked or a direct PC connection. In most cases a Hard Disk Drive on the target device is required to store the data needed for user authentication.

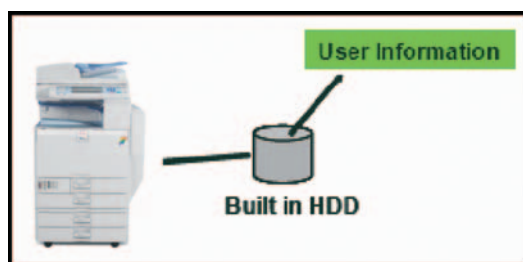
External Authentication Modes

- **Windows Authentication:** For customer networks using Microsoft Active Directory servers, this mode verifies the identity of the 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 device functionality. Using the same data that matches other areas of user network access eliminates the need for users to remember multiple passwords, and for IT personnel to support another login-password system. Once access is granted, the user's name is automatically entered in the Sender's Name field of outgoing Scan-to-Email jobs, providing traceability by eliminating "From" field spoofing.
- **LDAP Authentication:** Uses the company E-mail server to verify authorization in a manner similar to above, but for networks using a server other than Microsoft Active Directory. This mode permits or denies access to the entire device; it cannot control access to individual functions.



Internal Authentication Modes

- **Basic Authentication:** Limits device access by asking for a user name and password stored in the device's built-in address book. This allows customers to control device/data access in non-networked environments, and to limit access to stored files. 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 operator simply enters their User Code, which is compared to the registered data in the device's address book. No one without a valid User Code can access the machine. The same code can be used by multiple users to track system use by client, period, or by job for bill-back purposes, for example.



Ricoh Aficio Common Security Features Guide

In addition, when using Windows Authentication or the internal User Code function, it is possible to restrict access to specific features, such as whether or not to allow individual users and/or groups to print in color.

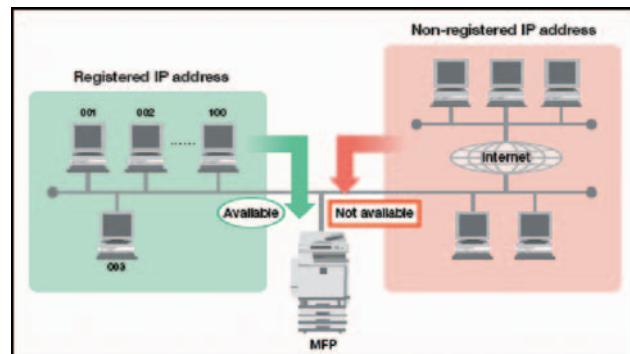


US Department of Defense Common Access Card (CAC) Authentication

The Common Access Card (CAC) is a US DoD specialized ID card-based authentication system design to make Ricoh MFP's 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].

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 an IP address 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.

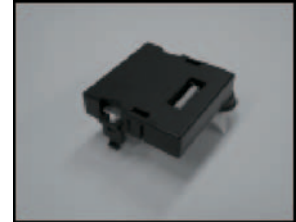


Job Logs / Access Logs

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, or whom and which device was used to send an unauthorized transmission to trace the source of leaks.

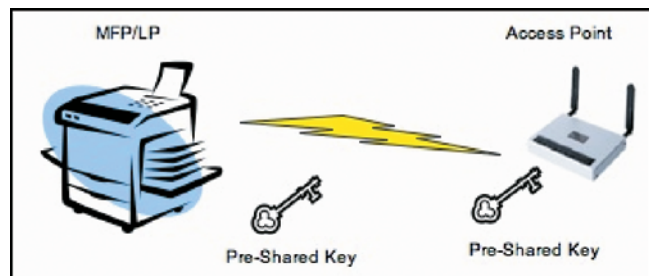
User Account Registration (User Account Enhance Unit)

Most Ricoh devices allow customers to register up to 30 user accounts to track and limit user access. Installing the optional **User Account Enhance Unit** increases capacity to a maximum of 500 accounts to monitor device usage and restrict larger populations' accessibility to printing functions. Printer usage data is saved so that it can be exported to an Excel spreadsheet for reporting/usage analyses.



WPA Support (Wi-Fi Protect Access)

Used in conjunction with the IEEE 802.11a/b/g Wireless LAN option, WPA is a new 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.

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.

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.

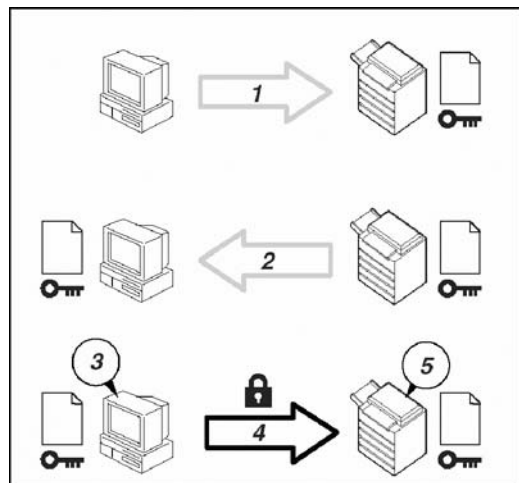
Ricoh Aficio Common Security Features Guide

Data Encryption

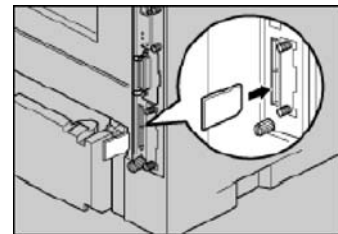
As mission critical data traverses the network it is possible for the knowledgeable hacker to intercept raw data streams, files, and passwords. The advent of wireless network technology, while increasing the convenience of surfing and printing for millions, also leaves networks vulnerable to attack from 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 Aficio devices are equipped with the following encryption capabilities to reduce these risks.

128-bit SSL/TLS (Secure Socket Layer/Transport Layer Security) Encryption & the Network Data Protection Unit

Once a user has been granted access to the device through an active authentication mechanism, Ricoh devices offer another level of security through password and data encryption capabilities. By scrambling data prior to sending it over the LAN for output or storage, it becomes impossible for hackers to decipher, and subsequently gain access to tamper or steal documents under false pretenses. A series of communications takes place between the sending PC and the printer or MFP so that passwords and/or data can be encrypted prior to sending, and decrypted once they arrive at the device. To enable this function, the Ricoh device must be equipped with the **Network Data Protection Unit**, and the **SSL Certificate** must be pre-installed.



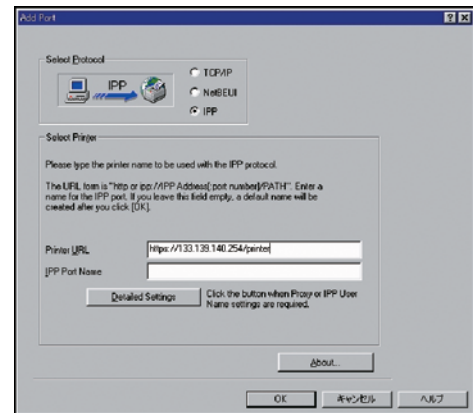
The Network Data Protection Unit (NDPU) is available as an option on some devices and is offered standard on others. The NDPU is installed in the main unit controller and employs 128-bit strength encryption to protect data. It works by dividing data sent from a PC over network lines into blocks of scrambled bits. This function can be activated when data is to be sent via the hardwired Ethernet interface, or the IEEE 802.11b Wireless LAN interface.



The SSL Certificate is a digital “key” that must first be installed on both the device and the sending PC via Web Image Monitor or SmartDeviceMonitor. Think of the SSL Certificate as an electronic credit card that verifies the user’s credentials and gives/denies permission to send data to a networked device in a way that cannot be understood or reassembled by anything other than the destination unit.

The NDP/SSL Certificate perform two functions:

1. **Encrypts entire files using the IPP** (Internet Printing Protocol) by reassembling scrambled blocks of data sent to it from a PC into proper order for printing.
2. Requires entry of an **encrypted password to print a PDF file**. The user must enter a corresponding password at the printer to output the file, or the print job will be cancelled.

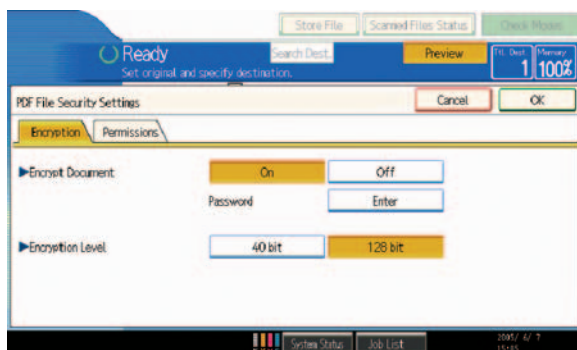


Address Book Encryption

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*.)

Ricoh Aficio Common Security Features Guide

Driver Encryption Key

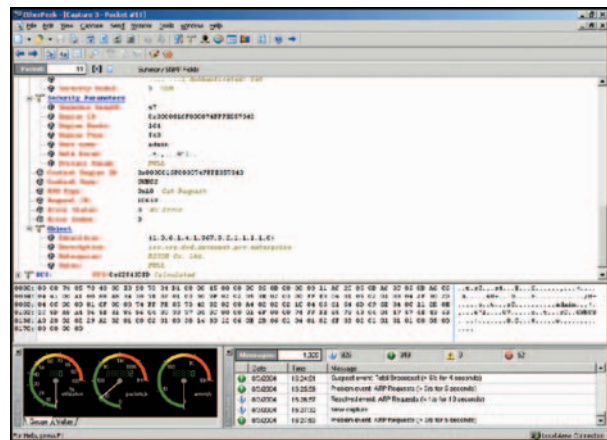
Ricoh devices offer this feature that scrambles user authentication passwords when using the PCL or RPCS drivers so others cannot access the system fraudulently using a stolen user's password.

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 (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 to maintain a secure environment.



Earlier versions (v1 and v2) of SNMP were used to configure and monitor remote devices. The latest version, SNMPv3, offers enhancements to user authentication and data encryption that deliver greater security features to protect customer data and network assets. When activated, SNMPv3 prevents unauthorized users from seeing either the password and/or the actual content of the file in readable text form, protecting valuable information.

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.

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.

Hard Drive (HDD) Encryption

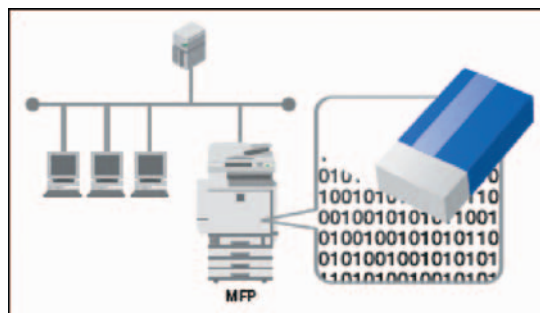
This function can encrypt the system's hard drive to protect against data theft. Even if the hard drive is stolen, data will not be disclosed. The encryption methodology used is Advanced Encryption Standard (AES) to 256 bits.

Document Protection

Finally, once a document has arrived at the output device for printing or storage, there needs to be sufficient protection in place to guard against unintentional access, reprinting, distribution, or modification for as long as the file resides in memory. Ricoh devices offer a number of features that safeguard information until the owner decides to retrieve or delete it.

DataOverwriteSecurity System (DOSS)

Ricoh devices with hard disk drives installed, sometimes referred to as the Document Server, temporarily store every document processed by Ricoh printers and MFPs whether copied, printed, faxed, or scanned. While there are considerable benefits related to sharing stored documents among authorized users, there is also the potential for unauthorized access, theft, or falsification. The DataOverwriteSecurity System (DOSS) eliminates these threats by overwriting the hard disk after each job so that files cannot be retrieved or recovered. Initially designed to meet government, military, and major account requirements for document security, you can use DOSS to add value to customers with all types of mission-critical documents that require protection from leaks and unauthorized distribution.



DOSS destroys temporary data (not documents stored to the Document Server or data saved in Address Books) stored on device hard drives using one of three overwrite methods. Overwriting not only applies to all copy and print jobs, but scanned files, Sample Print/Locked Print, and File Format Conversions as soon as the job is completed:

- NSA (National Security Agency) Standard: Overwrites the data three times: twice with random numbers and once with zeros.
- DoD (Department of Defense) Standard: Overwrites the temporary data with a fixed value, the fixed value's complement, and then with random numbers. It then verifies the result.
- Random Data Overwrite Standard: Allows users to overwrite temporary files with random numbers. Users select how many times the files will be overwritten, up to a maximum of nine times. The default is three times.

Ricoh Aficio Common Security Features Guide

When it is time to relocate or dispose of the system, an Erase All Memory function permanently erases all data on the HDD, including all files for long-term storage in the Document Server, Address Book information, user codes, additional fonts downloaded to the system, and network settings for ultimate peace of mind.

Ricoh currently offers several types of DOSS systems for use with different devices and hard disk drive sizes, ranging from Type A, B, C, D, F, H & I and achieved ISO 15408 Common Criteria Certification, a recognized worldwide standard that defines security requirements and establishes procedures for evaluating the security of IT systems and software. This certification provides your customers with independent, third-party validation of your device's security claims.

Locked Print/Secure Print

The Locked Print or Secure Print feature maintains confidentiality by suspending document printing until the authorized user enters a password at the device control panel that corresponds to a password set at the sending PC in the driver. This eliminates the possibility of anyone viewing or removing a confidential or sensitive document from the paper tray. The file is automatically deleted from memory after printing. Locked Print/Secure Print usually requires the presence of a hard disk drive, which may be optional depending upon the model. Password is now encrypted.



Locked Print Password Encryption

As a new feature the password used for locked printing can be encrypted to 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 protecting 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.

SmartDeviceMonitor (for Admin*)

SmartDeviceMonitor is utility software bundled with all printers, print-enabled MFPs and the Printer/Scanner Kit options. This versatile software suite simplifies all aspects of installation, monitoring and management of 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 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 output device.

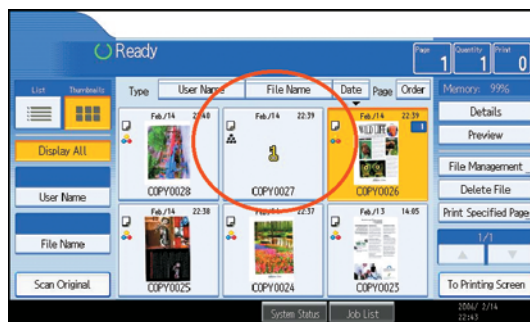
■ Restrict User Access

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 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.

**Note: SmartDeviceMonitor for Admin resides on the client desktop and allows users to determine the status and availability of networked peripherals. Once installed, an icon is placed on each user's desktop in the Windows Taskbar, which shows system status at a glance.*

Password Protection of Stored Documents

Any Ricoh device equipped with document storage capabilities can password-protect stored files. Users can set a password between 4 – 8 digits directly at the control panel to prevent other users from viewing, printing, or sending the file. In Ricoh MFPs equipped with Preview capabilities (pictured at right) documents assigned a password display a key icon instead of an image of the first page of the document to preserve confidentiality.



Ricoh Aficio Common Security Features Guide

RAM-based Security

Several low-end digital systems use RAM (Random Access Memory) for document processing tasks, not a hard disk drive. Though a hard drive may be available as an option, there is security benefit to non-HDD equipped systems in that jobs processed through RAM are volatile. This means that when power to the system is turned off, all temporary print data is immediately erased. Without a means to permanently store data, such as a hard drive, the security threat of unauthorized reprinting is eliminated. As such, RAM-only devices can be proposed for environments where information security is the top priority.

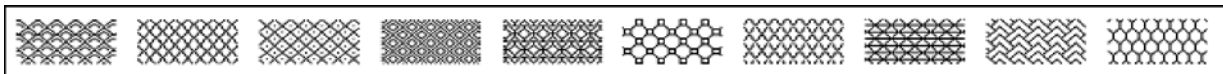
Removable Hard Disk Drive

Several Ricoh high volume MFPs offer the Removable Hard Drive option for ultra-security conscious customers. The **Removable Hard Drive (RHD)** option provides an ideal security solution for government, military, and other office environments that require high security. The system's internal hard drive is externally mounted in a secure bay, allowing the hard drive to be unlocked, removed and stored in a secure external location. To add an extra layer of security, an additional removable hard drive may be purchased to keep classified and unclassified information separate.



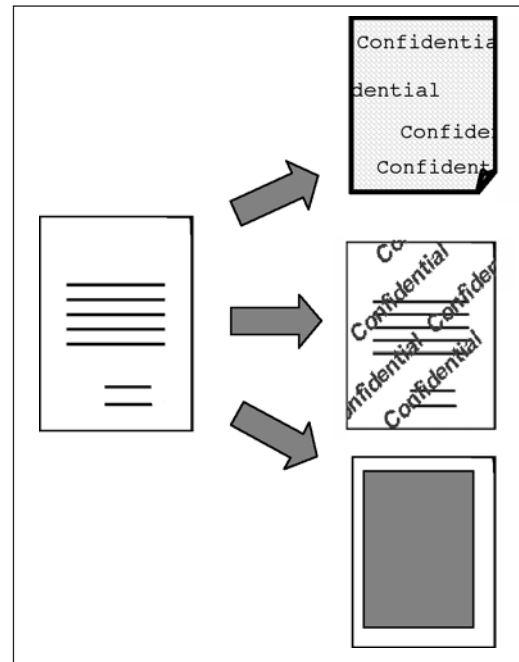
Unauthorized Copy Control/Masked Type

This function discourages the illegal copying of documents that were originally created and printed using the RPCS driver. When the optional Copy Data Security Unit is installed, files printed via the RPCS driver can be embedded with a special message that instructs the scanners of other Ricoh devices not to copy, scan, or send the page. Instead, page content is either grayed out, or overprinted with one of 10 possible obscuring patterns and/or a customized text message to deter illegal copying.



There are two modes:

- **Mask Type for Copying** is a standard RPCS feature that embeds a masking pattern and/or message within the original printout. If copies are made, an embedded message or the document originator's name appears on top of one of the selected masking patterns (shown above). Users can design the message just as they would a typical watermark.
- **Data Security for Copying** produces a page in which the entire image area is grayed out, making the document illegible.



Commercial Facsimile Security Solutions

Facsimile is included in this Security Solutions review as it remains a viable communication technology and Ricoh supports a complete line of stand-alone Super G3 laser fax solutions, as well as network fax systems and fax board options that can be installed within MFPs.

Even though a standard G3 fax unit utilizes digital scanning and printing it uses a modem for communication over a standard phone line. Since most standard phone lines are analog the modem converts the digital data to a format that can be sent over the analog phone lines. The receiving machine converts the analog data back to digital data so that the fax system can process and print it. Therefore, fax has a different set of security features and customers have a different set of questions for fax based solutions.

The most common question is whether a customer's data network can be penetrated via the fax connection on stand-alone fax system, network fax system, or an MFP with fax capability. The answer is NO. A Ricoh standalone fax, network fax or MFP with fax uses only a Class 1 modem that only controls fax transmission/reception. Regardless if fax is part of a network fax or an MFP connected to a network, the modem is physically separated from the main processor or any other network port. The fax modem cannot accept or understand any PDL or device command stream other than those conforming to established fax protocols, and therefore a data network cannot be breached via the fax modem.

Ricoh Aficio Common Security Features Guide

After you allay your customer's concerns about potential fax network threats, you can speak to a number of security features that are designed to improve basic faxing security in commercial fax environments. The following features apply to Ricoh stand-alone fax machines, network fax systems, and also to any MFP device that offers a Ricoh-engineered Super G3 Fax option.

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 faxes 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.

IP-fax

When the NIC FAX Unit is installed Ricoh facsimile systems support secure T.38 real-time IP-fax over a corporate Intranet. This not only bypasses costly phone lines, but also operates behind the firewall for secure point-to-point transmissions.

ITU-T Sub-address Routing

Using a Sub-address appended to a fax number (think of it like an extension on a business phone number), it is possible to route a fax directly to the recipient's PC via their e-mail address. When received directly to a PC, confidentiality is enhanced as the recipient can view the message and print a copy at their convenience.

Memory Lock

Similar to the Secure Print feature on a printer or MFP, when this feature is enabled documents from identified senders or all senders are retained in memory. Only after the Memory Lock ID is entered at the control panel will the documents stored in memory be printed, preventing transmissions from sitting unattended on a reception tray for passers-by to read until collected.

Restricted Access

Restricted Access allows customers to track and trace machine usage and deter casual passers-by from using the fax. Authorized users must enter a code before they can use the machine. Activity reports document the time and destination of every call. Further, this function can be linked to the Night Timer feature so that Restricted Access is activated during desired times to prevent after-hours access.

Security PIN Code Protection

To prevent accidental 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 LCD panel and activity report.

Server Domain Authentication

When security and user tracking are an issue for IT Managers, Server Domain Authentication limits fax access to users with a valid Windows domain controller account. Server Domain Authentication will limit access to the fax system not only for Scan-to-Email, but also for standard Super G3 faxing, IP faxing, and LAN faxing.

Wrong Connection Prevention

The machine will disconnect if the last four or eight digits of the dialed number do not match the CSI on the receiving machine.

Fax Security Compatibility Table

The following chart outlines the current Ricoh facsimile product line and those fax security features that are available with each product.

| | Commercial Facsimile Security Features | | | | | | | |
|---------------------------|--|-------------------------------------|--------|---------------------------|-------------|-------------------|------------------------------|------------------------------|
| | Closed Network | Confidential Transmission/Reception | IP Fax | ITU-T Sub-address Routing | Memory Lock | Restricted Access | Security PIN Code Protection | Server Domain Authentication |
| Super G3 Facsimile | | | | | | | | |
| FAX1180L | | ■ | | | | ■ | | |
| FAX2210L | | ■ | | | | | | |
| FAX3320L | ■ | ■ | | | ■ | ■ | ■ | |
| FAX4430L | ■ | ■ | | | ■ | ■ | ■ | |
| FAX4430NF | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| FAX5510L | ■ | ■ | | | ■ | ■ | | |
| FAX5510NF | ■ | ■ | ■ | ■ | ■ | ■ | | ■ |

Ricoh Aficio Common Security Features Guide

| Network Protection | | | Device Access | | | | | | | | | | Data Encryption | | | | | | | | | | Document Protection | | | | | | |
|--------------------|--------------------|--------------------------|------------------------------|--------------------|----------------------|---------------------------|---------------------|----------------------------|----------|-----------------------------|---|-----------------------------------|-------------------------|----------------------------|-----------------------|-------------------------|--------------------|--------------------------|---------------------|----------------|----------------------------------|-------------------------------------|---|---|---|----------------------|---------------------------|-----------------------|---------------------------|
| 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 |

Black & White Multifunction (continued)

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aficio MP 3500/P/SP/SPF/SPI/G | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 4001SP/MP 5001SP | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 4000B/4000/SPF | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 4500/P/SP/SPF/SPI/G | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 5000B/5000/SPF | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio 5500/SP | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio 6500/SP | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio 7500/SP | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 6000 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 7000 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 8000 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio MP 6001/7001/8001/9001 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio 2090 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio 2105 | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio Pro 906EX | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio Pro 1106EX | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Aficio Pro 1356EX | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Pro 907EX/1107EX/1357EX | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

