

Issued September 29th, 2011

Security White Paper
for
Streamline NX Version 1.2
Scan and FAX Manager

Solution Value Proposition Section
Global Technology Support Department
Service and Support Center
Global Marketing Group
Ricoh Company, Ltd.

Document version
SLNXSFMV1.2.0-1.0

Notice:

This document may not be reproduced or distributed in whole or in part, for any purpose or in any fashion without the prior written consent of Ricoh Company Limited. Ricoh Company Limited retains the sole discretion to grant or deny consent to any person or party.

Copyright © 2011 by Ricoh Company Ltd.

All product names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

Document version history:

Version	Date of Issue	Revision
1.0	September, 2011	1 st Release

1. INTRODUCTION	4
2. SYSTEM.....	5
3. NETWORK PROTOCOLS	6
3.1 PORTS AND PROTOCOLS	6
3.2 RECOMMEND PRECAUTIONS	9
3.2.1 HTTP COMMUNICATION	9
3.2.2 CONNECTING TO OTHER SERVERS	9
3.2.3 COMMUNICATION WITH ATTACHED DEVICES	9
3.2.4 COMMUNICATION BETWEEN SFM SERVERS	10
4. DATA FLOW & STORAGE	11
4.1 STORED DATA.....	11
4.2 DATA FLOW	13
4.3 SERVER/PC DATA.....	13

1. Introduction

This document describes potential network weak points and recommended precautions for them.

Ricoh products use network services to provide a variety of features for network clients, such as file sharing, printer sharing, HTTP services and also client services for accessing network servers running outside our products, such as an LDAP server or E-mail server.

As Ricoh products are designed for use inside an Intranet where network clients and servers are protected by firewalls, they rely on the Intranet's security policy, like the security provided by other network servers and clients. However, some customers require more strict security levels for network devices. This document focuses on providing the information necessary to protect against potential threats from external security risks and help customers to fit the Ricoh product into their security system.

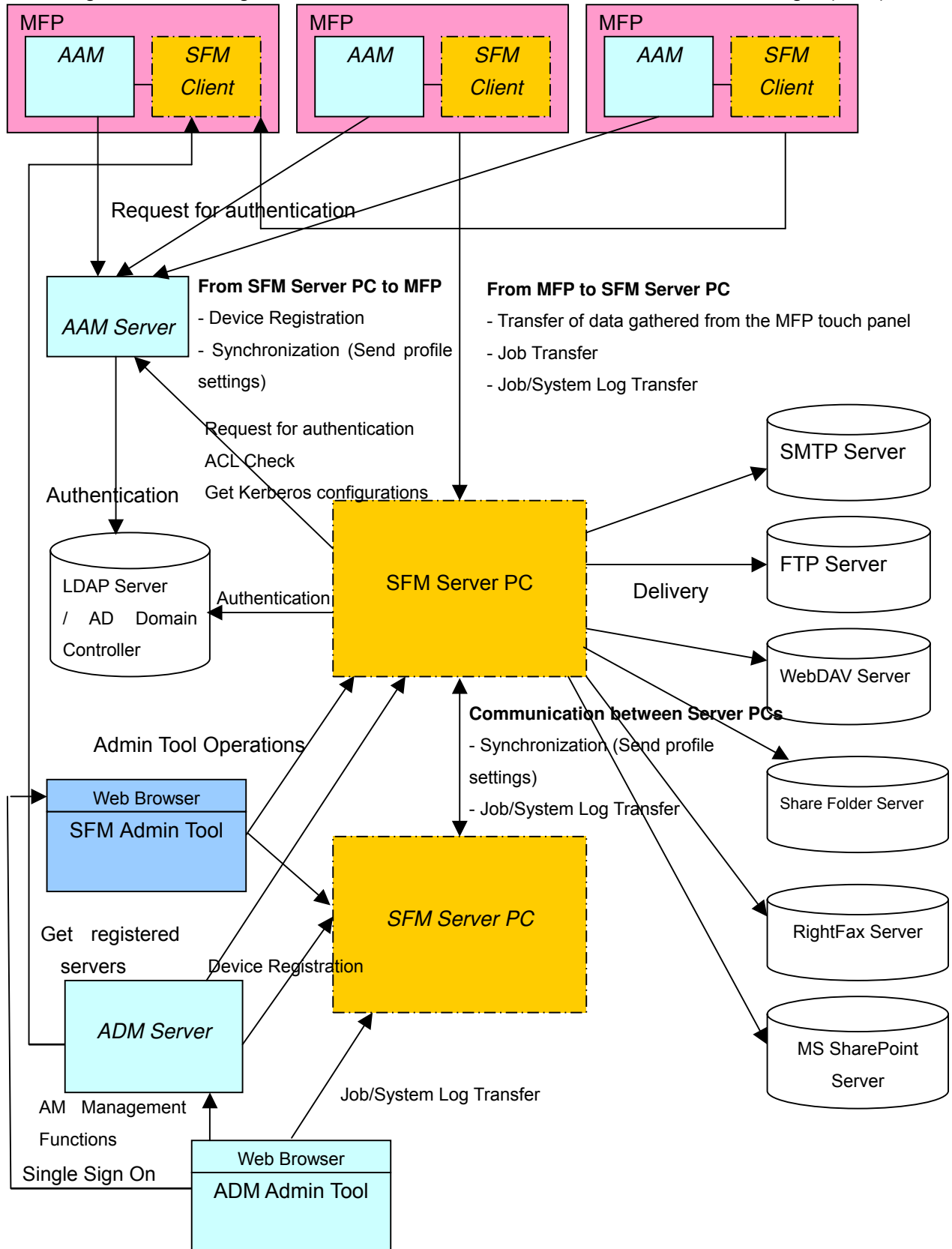
Ricoh products interact with non-Ricoh products, such as the operating system. If you are interested in learning about vulnerabilities in non-Ricoh products, please contact the vendor of that product.

Products and versions covered by this document:

Streamline NX Scan and FAX manager version1.2

2. System

These diagrams show the general data flow within Streamline NX Scan and Fax Manager (SFM).



3. Network Protocols

3.1 Ports and Protocols

The tables below describe the ports and protocols used for communication between the various parts of the SFM system.

SSL On/Off indicates the current SFM SSL configuration, as set by the SSL Setting Tool.

General Operations

Function	SSL Off		SSL On		Remarks
	Port	Protocol	Port	Protocol	
Admin Tool -> SFM Server MFP -> SFM Server	Set during install. (TCP)	HTTP	Set during install. (TCP)	HTTP	SSL Off: Default port is 8080. SSL On: Default port is 8443.
SFM Server -> MFP	8080(MFP) (TCP)	HTTP	51443(MFP) (TCP)	HTTP	Unable to change.

Individual Operations

Function	SSL Off		SSL On		Remarks
	Port	Protocol	Port	Protocol	
Log/Queue Operations SFM/ADM Admin Tool -> SFM Server	Set during install (TCP)	HTTP	Set during install (TCP)	HTTPS	
Device Registration ADM Server -> SFM Server SFM Server -> MFP	Set during install (TCP) 8080(MFP) (TCP)	HTTP HTTP	Set during install (TCP) 51443(MFP) (TCP)	HTTPS HTTPS	Used when synchronizing, etc.
Get Registered Servers ADM Server PC -> MFP	8080(MFP) (TCP)	HTTP	51443(MFP) (TCP)	HTTPS	
Get URL for Single Sign On ADM Admin Tool -> SFM Server	Set during install (TCP)	HTTP	Set during install (TCP)	HTTPS	
Authentication with AAM Server/ ACL Check /Get Kerberos Configurations SFM Server -> AAM Server	Set during install of AAM Server (TCP)	HTTPS	Set during install of AAM Server (TCP)	HTTPS	

Device Search

Function	Port	Protocol	Remarks
Device Search	161 (UDP)	SNMP	The port number is inherent to the SNMP protocol, and cannot be changed.

Load Balance Server / Secondary Delivery Server

Function	Port	Protocol	Remarks
Server Browsing SFM Server -> SFM Server	5353 (UDP)	Bonjour	Communication from the Main (Primary) Server to other SFM Server PCs.

Authentication (Retrieving Kerberos ticket from the Authentication Server)

Authentication Method	Function	Port	Protocol	Remarks
Active Directory	Authentication Process	88 (TCP, UDP)	KRB5	

Communication with Delivery Servers

Delivery Method	Port	Protocol	Remarks
E-mail Delivery SFM Server -> Email Server	25 (TCP)	SMTP/SMTPS	Set as part of Project properties, this port should match the settings of the SMTP server.
	110 (TCP)	POP	Used when POP before SMTP is used for authentication. Set as part of Project properties, this port should match the settings of the SMTP server. 110 is the default.
	389/636 (TCP)	LDAP/LDAPS	Set as part of Project properties, this port should match the settings of the LDAP server.
Folder Delivery SFM Server -> Share Folder Server	445 (TCP) 139 (TCP)	SMB	As a part of the JCIFS library, this port is unchangeable. When 445 is unavailable, 139 is used.
	137 (UDP)	NBNS	As a part of the JCIFS library, this port is unchangeable.
FTP Delivery SFM Server -> FTP Server	21/22 (TCP)	FTP/SFTP	This port should match the settings of the FTP server. Set as part of the Project properties, the port number is included in the URL of the Start Point Path. If a port is not specified, FTP's default is 21 and SFTP's default is 22.
	20 (TCP)	FTP	This port is automatically 1 less than the above port, and is not user-specified.
WebDAV Delivery SFM Server -> WebDAV Server	80/443 (TCP)	HTTP/HTTPS	This port should match the settings of the WebDAV server. Set as port of the Project properties, the port number is included in the URL of the Start Point Path. If a port is not specified, the default is 80.
RightFax Plug-in SFM Server -> FaxUtil (RightFax COM API)	-	COM	The COM API included in FaxUtil is used by the SFM server. RCL is not responsible for the communication between FaxUtil and the RightFax server.
SharePoint Plug-in SFM Server -> Microsoft Office SharePoint Server	80/443 (TCP)	HTTP/HTTPS	This port should match the settings of the SharePoint server. The port is set by adding the port number to the Start Point Path URL. If a port is not specified, the default is 80.
Send to Printer Plug-in SFM Server -> Printer Driver	-	-	SFM sends the print data to the printer driver using the standard Windows API. Communication between the printer driver and the printer is controlled by the settings in the printer driver.

RMI (Java Remote Method Invocation API)

Function	Port	Protocol	Remarks
Batch Execution	41108 (TCP)	JRMP	Batch Execution uses this port internally.
	41109 (TCP)	JRMP	Batch Execution uses this port internally.

Server Internal (Web server and servlet container)

Function	Port	Protocol	Remarks
Internal Communication	48009 (TCP)	AJP13	The web server uses this port for internal communication.

3.2 Recommend Precautions

3.2.1 HTTP Communication

Default communication between the AdminTool and the SFM server, and again between the SFM server and the MFP is done in HTTP without SSL and is therefore not encrypted. The password and other sensitive data are only protected by a weak encryption method. Users sensitive to security concerns should use SSL.

3.2.2 Connecting to other servers

Data sent between a SFM server and a resource server (FTP server, SMTP server, LDAP server, etc.), or an MFP and a resource server is also not protected by encryption. Users sensitive to security concerns should use SSL.

3.2.3 Communication with attached devices

Communication with devices occurs as follows:

(1) Device → SFM Server PC

- Transfer of data gathered from the device touch panel
- Job Transfer
- Job/System Log Transfer

(2) SFM Server PC → Device

- Device Registration/Synchronization (Send profile settings)

Using HTTP(S) as a base, data formats such as XML and CSV are sent and except for certain data (such as login credentials), this data is not encrypted. To maintain security, SSL is necessary. Also, when the MFP and SFM PC are separated and must pass through a VPN or NAT, address translation may not allow for correct operation.

3.2.4 Communication between SFM Servers

When using Load Balance or Secondary Delivery Servers, communication between SFM servers occurs as follows:

- Initial Load Balance or Secondary Delivery Server settings
- Server Browsing
- Server Synchronization
- Log Forwarding
- Job/Queue Operations
- Job Distribution between the Load Balance servers

Except for Server Browsing, default communication between the SFM servers is done over HTTP without SSL, and is therefore not encrypted. Passwords and other sensitive data are only protected by a weak encryption method. Users sensitive to security concerns should use SSL.

Information exchanged when Server Browsing is not encrypted because it does not contain any critical information.

4. Data Flow & Storage

4.1 Stored Data

Data	Item	Security Note
Profile Data	Access Control	Depends on Administrator Settings.
	Encryption	No Data Needing Encryption. ¹
	Back-up	Data saved in SFM's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	None.
	Remarks	
Project Data	Access Control	Depends on Administrator Settings.
	Encryption	No Data Needing Encryption. ¹
	Back-up	Data saved in SFM's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	None.
	Remarks	None.
Plug-in Data	Access Control	Depends on Administrator Settings
	Encryption	User IDs and passwords are encrypted using the 128-bit Blowfish encryption algorithm. The key used by the Blowfish algorithm is encrypted using the 1024-bit RSA encryption algorithm for communication on the network. ¹
	Back-up	Data saved in SFM's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	Depends on the Plug-in, but typically only failures are entered in the System Log, and both successful and failed operations are stored in the Job Log.
	Remarks	None.
System Settings	Access Control	Depends on Administrator Settings.
	Encryption	User IDs and passwords inside the Authentication Profile Settings and Administrator Settings are encrypted using the 128-bit Blowfish encryption algorithm. The key used by the Blowfish algorithm is encrypted using the 1024-bit RSA encryption algorithm for communication on the network.
	Back-up	Data saved in SFM's back-up system. Back-ups are created manually or using the Scheduled Backup function.
	Log Entry	It depends on the setting, but typically changes are written with an access record to the System Log.
	Remarks	None.

Data	Item	Security Note
Delivery job	Access Control	Administrators may see all jobs, while general users may only see their own jobs.
	Encryption	The User ID and password for login to a project are encrypted using the 1024-bit RSA encryption algorithm.
	Back-up	Delivery jobs remaining in the queue are not backed up.
	Log Entry	Success or failure is stored in the Job Log.
	Remarks	None.
Job Log	Access Control	Administrators may see all job logs, while general users may only see their own job logs.
	Encryption	Nothing encrypted.
	Back-up	The Job Log is not backed up.
	Log Entry	-
	Remarks	None.
System Log	Access Control	Only Administrators may see all system logs.
	Encryption	Nothing encrypted.
	Back-up	The System Log is not backed up.
	Log Entry	-
	Remarks	None.
Back-up Data	Access Control	Depends on Administrator Settings
	Encryption	Back-up data is encrypted when saved using Java's password-based encryption (PBE). If a password is not specified, the encryption is done using null characters.
	Back-up	-
	Log Entry	This and other maintenance operations are sent to the System Log.
	Remarks	Up to 30 instances of back-up data may be saved. A password can be set for an individual back-up data when it is downloaded, and that password must be entered when that same data is uploaded.

¹Profile, Project, and Plug-in data are all listed separately because SFM treats each set of data differently.

4.2 Data Flow

There are many network connections involved in the SFM system, and as those connections are done primarily in HTTP, the system is not very secure. Also, since SFM makes use of the FTP and SMB protocols when connecting with some resource servers, there are added weak points.

Users who feel that system is too weak by default should active the SSL settings to gain acceptable levels of security.

4.3 Server/PC Data

Except for some user information, such as account passwords, the server/PC resources such as the program data, configuration, registry, and logs are stored without encryption. There are no special protections on the stored data.

Therefore, special attention should be given to the server access, such as proper user access management, physical isolation, anti-virus software, etc.

End of Document